HACKER JOURNAL

Anno 1 - N. 11
24 ottobre/7 novembre 2002

Boss: theguilty@hackerjournal.it

Publisher: ilcoccia@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Karin Harrop

Contributors: Bismark.it, Tuono Blu, CAT4R4TTA, lupinIII, Enzo Borri

Cover
Libera interpretazione del logo della manifestazione tedesca PhotoKina 2002

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00187 Roma - Piazza Colonna, 361-
Tel. 06.69514.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

PAROLE, PAROLE, PAROLE

Dopo gli attacchi di Mafiaboy degli inizi del 2000, che misero in ginocchio per ore e ore Yahoo!, E*Trade, Datek Online e Buy.com, si disse che ora le piccole e grandi aziende dovevano assolutamente correre ai ripari e investire grandi quantità di denaro per rendere i propri sistemi più sicuri.

Dopo l'11 settembre, si è detto e scritto che la sicurezza sarebbe diventata la priorità di ogni organizzazione, pubblica o privata. Accanto al terrorismo, gli esperti cominciavano a delineare lo scenario della "guerriglia informatica", e quindi, insieme al rafforzamento della sicurezza per le strade e negli aeroporti, non si poteva più trascurare anche l'aspetto delle infrastrutture informatiche e delle telecomunicazioni.

"la sicurezza è un tema caldo, tutti vogliono sentirne parlare. Quando però si passa ai preventivi, poche aziende sono disposte a spendere quanto dovrebbero"

Poi, però, è scoppiata la bolla della "niù economy", i titoli in borsa hanno cominciato a calare. E questo ha fatto uscire parecchi armadi dagli scheletri di molte grandi aziende: false comunicazioni di bilancio, manager che si prendevano enormi quantità di denaro come provvigioni su guadagni mai realizzati... Insomma, per farla breve, un settore industriale in cui le centraliniste potevano comprarsi una casa con le azioni distribuite ai dipendenti, è diventato improvvisamente a corto di soldi da spendere. Dopo la pubblicità, una delle aree che ha subito i più pesanti tagli al budget è stata proprio la sicurezza, e in particolare la sicurezza informatica. E questo non avviene soli ai livelli più alti, dove si spostano milioni di euro (o dollari) come noccioline.

Nelle scorse settimane è stata presentato alla stampa Infosecurity, fiera dedicata alla sicurezza informatica, che si terrà a Milano dal 12 al 14 febbraio. Sono stati presentati i risultati di una ricerca eseguita da Sirmi, secondo la quale "più del 50% delle aziende italiane stanzia un budget per la sicurezza, e questa percentuale è destinata ad aumentare nei prossimi tre anni". Sarà, ma parlando con le persone intervenute, la situazione è apparsa piuttosto diversa: la sicurezza è un tema caldo, tutti se ne interessano e vogliono sentirne parlare. Quando però si passa ai preventivi, poche aziende sono disposte a spendere quello che dovrebbero. Certo, stanziano un budget per l'acquisto di un firewall, anche se magari poi lasciano le configurazioni predefinite. O comprano un antivirus per tutti i dipendenti, ma senza affidarsi a una società di consulenza che stabilisca delle policy per l'utilizzo del software e della rete aziendale. Insomma, la sicurezza è importante finché non bisogna tirar fuori dei soldi.

Vogliamo scommettere che quando avranno un problema con la sicurezza delle loro reti, queste stesse aziende reclameranno a gran voce una caccia alle streghe?

grand@hackerjournal.it

Saremo di nuovo in edicola Giovedì 7 Novembre!

Subject: Mi prende lo sfaso...

Scrivo a voi perchè voglio che più gente possibile legga le mie impressioni, ma non voglio rimproverarvi nulla, non avrei motivi.
Se volete potete anche non chiamarmi hacker. Io mi sono proprio rotto di quello sciame di wannabe del ca(vol)o che vogliono diventare "hacker" senza sapere nemmeno cosa voglia dire, solo per diventare famosi (?) o fare i figli con gli amici al bar. O per scopi che non tengono in minima considerazione l'orgoglio e la forza d'animo di quelli che negli anni 80 crearono il vero hacking.
È giusto che le irruzioni nei sistemi informatici siano considerate un crimine, ed è giusto venir perseguiti penalmente per questo. Se uno entra in casa mia senza permesso, io lo meno, qualunque sia il motivo che lo ha spinto a entrare. Basta nascondersi dietro a un dito.
I lamer ormai hanno contaminato la sensazione di puro orgoglio e stupore che mi aveva fatto avvicinare all'hacking; oramai la voglia di hackerare supera quella di voler imparare di tutto sugli argomenti che ci piacciono da dentro. E basta dare corda ai disadattati che usano internet per fare propaganda; basta lotte politiche sfruttando le debolezze informatiche, o danneggiare le persone che hanno la sola colpa di avere Windows e fregarsene di imparare a difendersi dalle stronzate del primo rincoglionito che a 15 anni crede di essere un divo solo perché conosce netbus. Prendersela con i più deboli è una cosa da perdente, da fallito, l'umiltà è invece una cosa che raramente trovo nell'undergound di oggi,anche se esistono ancora delle persone che meritano tutta la mia stima.
Meglio lo stereotipo di hacker con gli occhiali e i capelli arruffati che sta tutto il giorno davanti al pc per creare quello che la sua fantasia gli propone, che lo stronzo che irrompe nei sistemi per dimostrare qualcosa.
Una serie di coincidenze hanno purtroppo portato una cosa che stimavo a pieno in un' altra che mi fa inca@@are: giornalisti ignoranti, aziende che non capiscono un cax, e persone ingrate che sfruttano conoscenze di altri per i loro scopi del ca**o, o quelli che solo perché hanno Linux si sentono superiori ai "mortali" con windows.
Internet sta prendendo un potere enorme, superiore a tutti i media, e l'hacking è visto come il lato cattivo di internet, e per questo tutta quella manica di stronzi cisi ficca dentro, distruggendo quello a cui io credevo veramente, manuali per fabbricare bombe, tutorial su come rubare sulle cose più disparate ma che chiappe significa, anarchici dappertutto, OOHHH?.
L'hacking deve esistere, serve a tutti, ma ormai il vero significato di questa parola pochi lo conoscono.
Potete insultarmi o dirmi quello che volete, dirmi che non capisco un caxxo, ma non cambierete quello che penso.

Genocid3

> "L'hacking deve esistere, serve a tutti, ma ormai il vero significato di questa parola pochi lo conoscono".

> "Internet sta prendendo un potere enorme, superiore a tutti i media, e l'hacking è visto come il lato cattivo di internet"

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE MID HACKING HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

mailto:
redazione@hackerjournal.it

LETTERA O SFOGO?

La lettera a firma di Loxeo riguardo alle sue disavventure coi defacement mi ha veramente colpito e allo stesso tempo amareggiato. Ormai il panorama della rete è pieno di questi personaggi veramente ignobili per non dire di peggio. Io lavoro in una ditta che fornisce servizi di hosting, e in questo anno un paio di defacciamenti ci sono stati, ma non è questo il problema. Mi sembra però che il 90% di quelli che in rete si definiscono "hacker" realmente sono dei coglio....
E di questo mi sono convinto con questo episodio: un giorno ci chiama un cliente e mi segnala il defacciamento. Visto che si è capito il sistema che era stato usato per entrare , ma poi gli chiedo se gentilmente posso sperimentare quello segue e cioè non operare nessun accorgimento per evitare l'intrusione, per vedere come andava a finire. Lui acconsente e, per farla breve, lo stesso "imbecille" defaccia il sito per una settimana. Allora mi chiedo: che gusto c'è in tutto questo???
Posso capire la prima volta ma le altre 6 di seguito che soddisfazione portano? Tra le altre cose sicuramente il mio amico è passato dalla parte di quelli che odiano questi fantomatici "hacker".
Alcune volte bisogna pensare che molti lavorano grazie al sito internet e magari non tutti possono capire come arginare questi defacciamenti, e di conseguenza possono magari perdere quello che con tanti sforzi si sono costruiti, per colpa di questi cerebrolesi.
Riflettiamo anche su come si naviga oggi e cioè con il firewall, l'antivirus, l'antispyware, l'antidialer e l'aspirina per il mal di testa :-) E poi dicono che la rete è libera, forse 10 anni fa lo era, ormai solo per entrare in rete devi corazzarti peggio che se stai andando in guerra. Sinceramente, alcune volte tornerei indietro, per certi versi. Forse più che una lettera è stato uno sfogo e mi scuso di questo.

ZAK

D'accordo su tutta la linea, tranne che su un punto (hum... quante metafore "geometriche"). Dici che un operatore di servizi Internet potrebbe anche non sapere come rimediare a un defacement; beh, questo è un po' grave. La messa in sicurezza del suo server dovrebbe essere una delle sue priorità, e se non sapesse come fare, allora è meglio che cambi mestiere. Del resto, un server insicuro è un problema per l'intera comunità della Rete (perché da lì si possono lanciare attacchi, inviare spam, fare danni...).
Con questo non voglio giustificare chi defaccia un sito, ma suddividere un po' le responsabilità tra chi agisce da vandalo, e chi non prende le precauzioni che dovrebbe.

PERCHÉ PARLARE DI TROJAN?

Dai titoli sulla copertina vedo che negli ultimi due numeri avete parlato di SubSeven e NetBus: quella è roba da lamer! Perché trovano spazio sulla vostra rivista?

C0D3D

Siamo perfettamente d'accordo sul fatto che i trojan siano roba da lamer. E se non ti fossi fermato alla copertina, ma avessi letto il contenuto degli articoli, avresti capito al volo che si tratta di schede che descrivono i rischi e spiegano come identificare e rimuovere i server di queste backdoor dalla propria macchina.

ROCK TAROCCO.

Aosta, un giorno di settembre, edicola solita... compro il vostro giornale, un po' per abitudine un po' curiosità leggo subito l'articolo su Rocco Tarocco. Ho lavorato in discoteca (deejay e non buttafuori... :-P) per 15 anni di musica ne ho tonnellate (tra lp, mix e i gloriosi 45 giri). Trovo di una stupidita estrema la pubblicità della universal (volutamente con la u minuscola)... Trovo stupido ed estremamente indecente che un cd costi 20 euro. Ho sempre comprato musica (anzi compravo) adesso tutto ciò che ho dal 99 in avanti è scaricato salvo (lo so sono un sentimentale) qualche autore (vedi Vasco) a cui regalo volentieri i miei dindini, per via delle emozioni che mi ha regalato e che mi regalerà ancora.
Trovo vergognoso che una persona come Piero Pelù in un intervista su Rockerilla di qualche annetto fa dicesse "i Litfiba non faranno mai musica commerciale". Complimenti! E che dire sul nostro amico, il compagno Jovanotti: un suo concerto a 30 euro. Complimenti anche a te.
Lo sfogo era ed è volutamente aggressivo. Care case discografiche, volete sconfiggere la pirateria? Abbassate i prezzi dei CD, e non solo di quelli che avete venduto 5 anni fa. Il budget lo fate con i titoli nuovi, e non venitemi a dire che il problema è l'artista, perché con una chiacchierata e un esame di coscienza di tutto l'ambiente musicale, uno sforzo congiunto genererebbe solo del bene per chi li compra i cd e per chi li fa....
Altrimenti io come tanti altri, di mp3 ne scaricheremo a tonnella-

Questa è di Badboy84, al quale deve essere piaciuta la frase del logo dell'Hack Meeting (www.hackmeeting.it).

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

SULLA SETTA CINESE

Vi scrivo riguardo alla notizia sulla "setta" Falun Gong a pagina 10 del numero 9. Lo so che non siete un giornale di informazione, ma dovete sapere che gli appartenenti a quella setta, in Cina, sono perseguitati con tutti i mezzi illeciti che possano venire in mente a un essere umano: oltre al "classico" carcere (per un numero di anni sproporzionato, e senza alcun contatto con il mondo esterno), si parla di torture e reclusione in manicomio (della qual cosa si sta occupando la World Psychiatric Organization). E non si tratta di una setta che "copra" un'organizzazione criminale: il motivo della repressione è puramente ideologico (così come non sono ben visti -eufemismo- i cattolici). Quello che non mi è piaciuto, dicevo, è che invece di mettere quella fotona di un satellite che non c'entrava nulla, potevate mettere due righe per ricordare che, per quanto ne sappiamo noi in Italia, il governo cinese non ha un motivo lecito per perseguitare gli appartenenti a Falun Gong. E, del resto, azioni di pirateria come quella da voi riportata sono l'unico modo che la setta ha per fare propaganda all'interno del proprio paese. A meno di non esporsi e diventare martiri in poche ore. Avete accennato qualche volta all'"hacking" di cervelli. Be', un'informazione parziale, come ben sapete, permette a chi la elargisce di aprire molte più falle di sicurezza nei cervelli dell'uditorio (di prenderne il controllo, letteralmente), rispetto ad un'informazione completa. Una battaglia che per voi è solo un satellite rapito, per altri significa vita o morte.

STM

te... e non preoccupatevi che per ogni buco che chiudete (software bandito, server chiuso...) se ne apriranno altri 10

CUCCIOLO1966

Il punto è che anche comprando i dischi, nella maggior parte dei casi i soldi non arriveranno mai all'artista. I produttori li trattengono come risarcimento per il servizi di promozione. Chiunque non sia uno dei "grandi" della musica, che può vivere di diritti d'autore, i soldi li fa coi concerti. Peccato che però se nessuno compra i primi dischi di un gruppo emergente, difficilmente ne verranno prodotti altri.... Stiamo ancora aspettando che la Rete diventi un vero canale alternativo alla distribuzione e promozione artistica e musicale.

LA MUSICA NON È GRATIS

Vi scrivo riguardo al sondaggio che avete fatto sullo scorso numero di HJ e, scusate se ve lo dico, ma a questo punto vi reputo dei gran "pulciari". Io mi trovo in assoluto disaccordo con l'esito che questo sondaggio ha avuto e a questo proposito vorrei fare una domanda a tutti: gli strumenti COSTANO, i concerti COSTANO, le registrazioni a questo mondo viene dato in maniera completamente gratuita e allora, io che sono un musicista vi chiedo, COME SPERATE DI FAR ANDARE AVANTI LA MUSICA SENZA UN CENTESIMO?

LORENZO

Occhio a non scambiare l'opinione dei lettori, espressa tramite il sondaggio, con il punto di vista della rivista (che credo sia emerso abbastanza chiaramente sulle pagine del n. 10, e non si discosta molto dal tuo).

ASSISTENZA REDHAT

Ho deciso di istallare Linux (Redhat 7.1) sul mio portatile; dopo l'installazione ed il riavvio mi ritrovo con un errore in X "Fatal IO error 104 (Connection reset by peer) on X server ":0.0" after 0 requests (0 known processed) with 0 events remaining." Questo è l'errore, io non conosco Linux ma mi sembra di aver capito si tratti di un problema di configurazione di X. Ho provato diverse soluzioni con Xconfigurator ma non ho ottenuto risultati.
Ora, sicuramente direte: "Potresti rivolgerti a Redhat!" Già fatto; mi hanno risposto "Errata configurazione X" Questo già lo immaginavo, ma non mi hanno dato altre info...
Non voglio fare polemica, sicuramente avranno un sacco di rompiballe come me, ma non mi sembra il modo di trattare un cliente visto che osannano il loro servizio assistenza. Non nascondo la mia delusione: pensavo che acquistare un "buon Linux" fosse una buona idea, ed invece è una guerra.

WILLY

Tu non vuoi fare polemica, ma io sì. Se hai acquistato e registrato la distribuzione, e questo è tutto quello che ti hanno risposto, è un pochetto scandaloso, visto che il prezzo del pacchetto è costituito in larga parte dal servizio di assistenza. Qualcun altro ha avuto esperienze simili? RedHat vuole far sentire anche la sua campana? (Willy ha risolto il suo problema chiedendo aiuto nel canale Irc #hackerjournal su irc.azzurra.it).

HARD DISK CONGELATI?

Volevo esprimere qualche perplessità circa la lettera di Simone pubblicata nella rivista n. 8. Bene, l'amico ci parla dei suoi accostamenti precoci all'informatica e comincia a sparare a zero su gente "che crede di saperlo usare perché ha il PC potente o perché parla strano" e poi spara la cazzata del congelamento degli Hard Disk... So che questa

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: sk8ing
pass: hj4u

MEMORIA FALLIBILE

Salve amici! Ho un problema e mi chiedo se potete risolvermelo o almeno darmi qualche spiegazione: quando accendo il mio PC mi capita a volte di leggere alla prima schermata, subito dopo che ha caricato la ram, la scritta: MEMORY TEST FAIL. Potreste darmi qualche spiegazione?!

I programmi residenti nel Bios hanno fatto un test della memoria, ed è risultato qualche problema. Forse si tratta di un banco inserito male, o difettoso. Ma può trattarsi anche di un problema del firmware della scheda madre: prova a verificare se esistono per il tuo modello degli aggiornamenti del Bios (procedi con cautela, seguendo attentamente le istruzioni: potresti rendere il PC non più utilizzabile se sbagli qualcosa).

non è una rivista scientifica, ma inviterei questa persona a riguardare qualche libro di scienze delle scuole medie e leggere qualcosa sulla termodinamica e i passaggi di stato. Infatti, per quanto io ne sappia, i piatti negli HD sono posti a condizioni fisiche particolari dove le leggi della termodinamica non sono del tutto rispettate e non solo... qualora si passasse dallo stato aeriforme a quello solido (che non è il congelamento!) e poi tramite il calore sprigionato dal funzionamento dell'HD si passerà dallo stato solido a quello liquido e quindi in presenza di quest'ultimo l'HD si scassa e lo dobbiamo buttare.
Volevo precisare che questo non è un attacco personale all'amico, che sento come un fratello vista la passione che ci lega, ma volevo solo chiedere di non far di tutta l'erba un fascio!

Secondo me hai preso un po' troppo sul serio la faccenda. Quando Simone diceva "congelati", probabilmente non lo intendeva in senso letterale, ma come uno ha freddo e dice "sto gelando". È ovvio che nella camera dove ci sono i piatti, non può gelare nulla perché è sotto vuoto. Il freddo intenso può però bloccare il motore o comunque portare a malfunzionamenti. Non a caso, le specifiche di molti hard disk parlano di una temperatura di utilizzo da 5 a 55 gradi. Come vedi, non c'è bisogno di scomodare la termodinamica e i passaggi di stato.

CD RADIOATTIVI?

Egregia redazione,
volevo avere delle informazioni riguardanti alle radiazioni del lettore cd. Come è noto vi è un adesivo sul lettore dove vi dice di non aprire il lettore cd perché ci si può irradiare, da cosa e in che modo? Il motivo però della mia mail è sapere se smontando il lettore cd con il computer smontato e privo di corrente, si possa incappare nelle radiazioni.
GIOVANNI M.

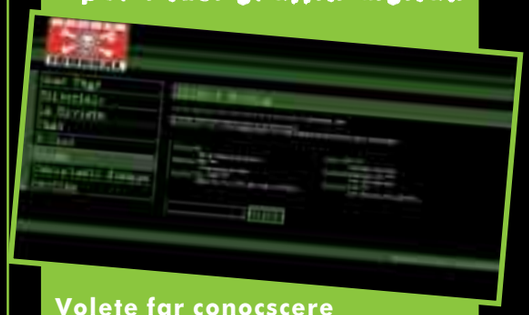
Tranquillo: si riferisce alla radiazione luminosa emessa dal laser, insomma alla sua luce. Se puntata direttamente negli occhi, può danneggiarli seriamente. Ovviamente questo non accade nell'utilizzo normale di un CD o di un masterizzatore, perché il raggio laser è all'interno dell'involucro. Se però smonti le protezioni e poi accendi l'apparecchio, puoi seriamente danneggiare i tuoi occhi o quelli di qualcun altro, anche "apparentemente" molto lontano.

HACKER=CRIMINALI

Oggi ho letto sul giornale che un gruppo di Hacker ha rubato 15.000 euro di merce (Dvd, PlayStation eccetera) orinandola da altri paesi, e alla fine li hanno beccati solo perché sono andati a recuperarla personalmente. Sì, sono stati così stupidi a non pensare un piano per ritirare la roba, ma almeno loro ci hanno provato e per quanto riguarda l'ordinazione della roba ce l'hanno fatta. Detto questo, dico una cosa a tutti gli aspiranti Hacker, essere un pirata elettronico vuol dire essere un criminale (addirittura l'Hacker governativo viene paragonato ad un terrorista proprio come Bin Laden) e se non siete capaci di fare i criminali, allora lasciate stare. Quindi riflettete prima di dire <Hacker è figo!>. Perché nessuno vuole solo le parole, nessuno vuole persone che diventino Hacker per mandare virus agli amici tanto per scherzare; vogliamo Hacker seri e non fasulli: vogliamo criminali!
TINX

L'unica fonte di dispiacere che ho nel fatto che quei truffatori sono stati arrestati, è che hanno (ulteriormente) gettato fango sul mondo hacker. Per il resto, non mi dispiace che li abbiano presi. Così come non mi dispiacerebbe se per via di questa risposta, tu smettessi di leggere Hacker Journal.

Hackerjournal.it, il muro per i tuoi graffiti digitali



Volete far conocscere il vostro sito, o semplicemente segnalare una risorsa che può essere utile a tante altre persone? Inseritela nella sezione Links di Hackerjournal.it

Organizzati in categorie, troverete decine e decine di siti, con una breve descrizione del contenuto per trovare subito quello che cercate (è comunque presente anche una comoda funzione di ricerca).
Un'ultima cosa... evitate di inserire siti che non hanno a che fare con tecnologia e hacking: verrebbero scartati dalla redazione.

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

SQOLA: SE TOGLI LA Q, SI LEGGE "SOLA"

Ho deciso di scrivervi per cercare di rispondere, o meglio, di ampliare il discorso iniziato nella lettera di Francesco (hj numero 7) e continuato da Alessandro nel numero 9. Io sto attualmente frequentando la 3ª liceo scientifico di tipo Pni (Piano Nazionale dell'Informatica, ed il nome è tutto un programma). Ho scelto questo indirizzo perché sono sempre stato attirato dalle materia scientifiche e soprattutto dall'informatica; e poi ho pensato "in un pni mi insegneranno ad usare meglio il pc, seno nn gli avrebbero dato quel nome, giusto???" Ed invece no, hanno preso per i fondelli: altro che informatica ed informatica, in tre anni non ci hanno mai portato 1 VOLTA nell'aula che sarebbe stata adibita a questo scopo! Io, ed altri studenti avevamo chiesto informazioni al preside dell'istituto e questo non ha fatto che confermare che il nome è tutta una bufala, ha ammesso che per pni si intendono solo qualche ora in più all'anno di matematica. Si che è la base dell'informatica, ma almeno un'oretta al mese ci possono portare, o no? Così, deluso da questa notizia, in prima ho frequentato un corso di "informatica" che spiegava l'utilizzo di windows, word, excel, powerpoit. Nei primi due nn avevo problemi ma con i rimanenti ero piuttosto carente. Ho messo informatica fra parentesi perché in realtà quello era un corso di paleontologia: il computer dell'insegnante era uno sfavillante Pentium mmx 200, mentre le nostre postazioni erano dei mostruosi Pentium 133. Naturalmente l'os era winzoz, ops... windows 95 mentre office era in versione 97. Naturalmente quando si voleva accendere il reperto e far partire office, si poteva fare un giro in bagno e ritornare dopo mezz'ora, per ritrovarsi la macchina che stava ancora macinando... E così col passare del tempo la mia delusione aumentava sempre di più, poi all'inizio di quest'anno la presa per il c**o è arrivata all'apice: ci è stata proposta la possibilità di ottenere una patente europea dell'informatica (non ricordo il nome preciso) , pagando ben 300 ; bisogna svolgere 7 esami riguardanti windows e i vari programmi della suite office... Per me la cosa più strana è che in un mondo in cui ogni mese (se non ogni giorno) vengono messi sul mercato nuovi programmi, loro mi insegnano ad usare windows 95! Ma cosa me ne faccio di un os di 7 anni fa!!! Va bene, non posso pretendere che abbiano l'xp, ,ma almeno un Me ci starebbe bene! Poi secondo me potrebbero anche installare linux, giusto per ridare un minimo di vitalità a quei PC. Con questo è da tempo che io ho smesso di aver fiducia nelle istituzioni pubbliche, se si vuole imparare bene qualcosa o si fanno dei corsi specifici (ma non alla mia età) o si studia da autodidatta con guide web e manuali.

..:: < Vender > ::..

SATELLITE VS ADSL

Scrivo a proposito della news pubblicata sul numero 10 di hacker journal: "ADSL SI ADSL NO" nella news scrivete: "Il divario diventerà ancora più netto con l'ampliamento della banda a disposizione delle persone raggiunte dal servizio, e ancora più netta sarà la differenza tra quelli che ormai si ritengono italiani di serie b".
Vorrei specificare che i cosiddetti "italiani di serie b" non sono costretti a dover scegliere come provider l'Adsl di Telecom o di altri operatori, ma esistono servizi (Netsystem) che permettono, pagando un minimo canone di avere l'ADSL anche negli 8100 punti non raggiunti dall'ADSL.
Come ben si evince le possibilità ci sono, basta saperle scegliere.

GiOvO

Vero, ma non troppo. NetSystem ha in effetti un paio di problemi. Innanzi tutto, richiede comunque un collegamento con modem su linea telefonia (e questo fa sì che tu debba pagare un tanto al minuto, cosa oltre alla maggiore lunghezza di banda, è uno dei più importanti vantaggi di Adsl). Poi, la velocità è molto variabile. È molto veloce con quei siti/file che sono presenti nella sua cache (i più visitati/scaricati dagli utenti). Con gli altri siti, è solitamente più lenta di un'Adsl completa. Ciò non toglie che in molti casi il collegamento satellitare può essere un'alternativa per chi ha come opzione solo i collegamenti dialup.

PROPAGANDA VIRALE

Tempo fa girava un "virus" che tramite Outlook prendeva un pezzo di qualsiasi documento di testo dal PC, poi dalla rubrica di Winzoz (Windows), prendeva gli indirizzi e mandava questa sorta di mail a tutti quelli che erano inseriti nella rubrica stessa! Il risultato finale era una mail con un pezzo di testo senza significato e naturalmente lo stesso "virus" (non visibile) che continuava questa sorta di catena di S.Antonio non voluta. Sarebbe possibile usare questo tipo di "virus" per propagare una mail contenente sempre lo stesso testo? Esiste un sito web dove possa reperirlo? Tutto questo mi serve per far circolare una mail senza usare una catena che tanto non verrà mai portata avanti!

titto8

FERMO LI'!
Quello che chiedi è inanzi tutto scorretto dal punto di vista della netiquette, che condanna la propagazione di mail non richieste, e l'impiego di worm e virus, per qualsiasi motivo.
Secondariamente, ma non meno importante, la diffusione di virus è un reato penale piuttosto grave.
Cose simili non si fanno, perché non puoi prevedere gli sviluppi, e consumeresti risorse, banda e tempo di molte persone per i tuoi scopi, anche se nobili.
Se hai idee o progetti da diffondere e propagandare, trova altri modi: frequenta liste e gruppi di argomento affine, crea un sito, scrivi una lettera mirata... ma lascia perdere i virus e le catene.
L'unica cosa che otterresti sono le maledizioni di migliaia di persone, la cancellazione dell'account da parte del provider e l'attenzione "particolare" delle forze dell'Ordine.

NEWS

HOT!

CAVALLO DI TROIA IN SENDMAIL

Il CERT/CC rende noto che **in alcune copie dei codici sorgenti del mail-server open source Sendmail è contenuto un cavallo di troia**. La versione in questione sarebbe la 8.12.6 e distribuiti dal 28 settembre al 6 ottobre 2002. Il trojian apre la porta 6667/tcp: il consiglio per tutti è quello di ricompilare Sendmail o filtrare la porta in questione.

L'80% DEI COMPUTER IN CINA È INFETTO

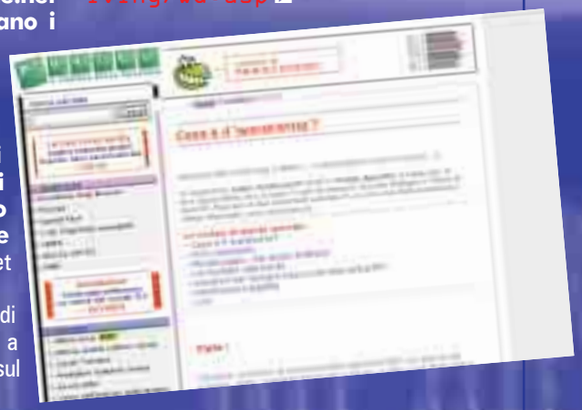
Il quotidiano "China Daily" riporta i risultati di uno studio condotto dal Centro nazionale di emergenza per i virus da computer. Zhang Jian, uno dei ricercatori che ha condotto lo studio, afferma che **"solo il 16% degli utenti di computer non è rimasto vittima di un virus quest'anno"**. Metà dei computer infetti ha perso dati.

SMAU ITALIAN LAN PARTY

A Smau, nel Padiglione 9/2-Ingresso Porta Metropolitana da giovedì 24 a Lunedì 28 Ottobre . Sono queste le coordinate per chi è interessato a **partecipare al più grande torneo del genere mai organizzato in Europa**. Gli appassionati del multiplayer potranno cimentarsi nei più famosi giochi in circolazione come: Quake 3 Arena, Half Life Counter-Strike, Return To Castle Wolfenstein, Medal of Honor, Jedi Knight II, Tribes, Age of Empires II, Starcraft Broodwar, Fifa World Cup 2002. Per informazioni e per l'iscrizione www.smauilp.it.

INCHIESTE SULLE RETI WIRELESS APERTE

I sorrisetti che accompagnavano i racconti di scorribande per le città alla ricerca di reti wireless sprotette, da segnalare col gessetto sul marciapiede, stanno lasciando il posto alla preoccupazione. Da fenomeno di colore, il wardriving di sta trasformando in attività organizzata, grazie a **siti come consume.net o seattlewireless.com, che mappano i punti di accesso aperti**, e invitano apertamente i possessori di un punto di accesso a non applicare protezioni. Quello che di solito non si dice, è che così facendo ci si espone al **rischio di essere ritenuti responsabili di eventuali realti che uno sconosciuto potrebbe compiere** sfruttando la connessione Internet gentilmente resa disponibile.
Anche dalle nostre parti, la presenza di punti di accesso non protetti comincia a preoccupare. Una interessante indagine sul campo svolta a Milano da Naif e Vodka per conto di Portel ha portato a **individuare in un'ora ben 18 punti di accesso, dei quali 12 senza protezione Wep**. L'articolo con le modalità e i risultati dell'inchiesta è su www.portel.it/wireless/wardriving/wd.asp

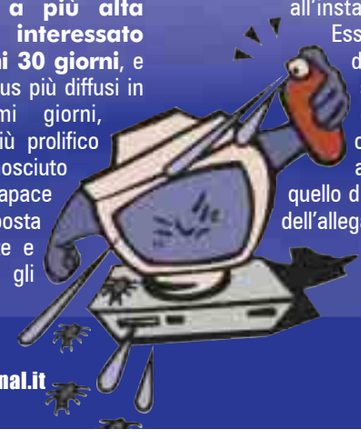


ETICA HACKER A SMAU02

Quest'anno a SMAU, all'interno dell'area dedicata alla sicurezza informatica, verrà dato grande spazio allo "Ethical hackers' speech" organizzato dagli Italian Blackhats (**www.blackhats.it**). Blackhats.it , come possiamo leggere nella presentazione del loro sito, "è una comunità di ricerca sorta spontaneamente, formata da un gruppo di persone tra i quali hackers, esperti di security, alcuni che lavorano nel mondo dell'I.C.T., altri impegnati come ricercatori. **Professionisti della sicurezza informatica, con forti legami al mondo underground e alla filosofia hacker**, che si dedicano all'innovazione tecnologica ed al miglioramento della sicurezza della rete Internet. Lo fanno per proprio conto e con risorse proprie, dedicando il tempo personale a questa passione…". **Social engineering, sicurezza del web, attacchi man in the middle e crittografia sono solo alcuni degli argomenti che verranno trattati quest'anno**. È comunque possibile rintracciare il programma completo dei Blackhats all'indirizzo www.blackhats.it/eventi/26102002/programma.pdf o maggiori informazioni sulla manifestazione SMAU all'indirizzo www.smau.it.

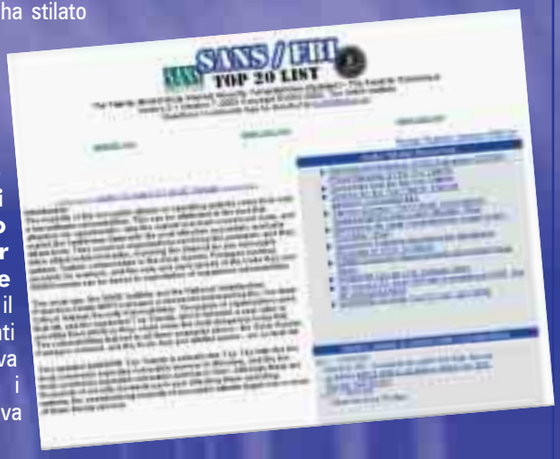
WORM BUGBEAR: IL VIRUS PIÙ PROLIFICO DI TUTTI

Secondo il servizio di monitoraggio di McAfee, **Bugbear è primo nella classifica dei virus a più alta diffusione che hanno interessato l'Europa durante gli ultimi 30 giorni**, e secondo nella classifica dei virus più diffusi in Nord America negli ultimi giorni, diventando di fatto il virus più prolifico degli ultimi 6 mesi. Il virus, conosciuto anche con il nome Tanatos, è capace di diffondersi attraverso la posta elettronica, condivisioni di rete e sistemi P2P. Molteplici sono gli effetti per chi è contaminato: dalla memorizzazione di quello che viene digitato all'installazione di backdoor. Essendo il soggetto e nome del file variabili, l'unica speranza per accorgersi della presenza di Bugbear, oltre che tramite un ottimo antivirus aggiornato, è quello di controllare la dimensione dell'allegato che è nella stragrande maggioranza dei casi 50.688 byte.



I 20 BACHI PIÙ FREQUENTI? È L'FBI CHE CE NE PARLA

L'FBI, congiuntamente ad amministratori di sistema di molteplici nazionalità, ha stilato la classifica dei 10 bachi maggiormente presenti nei sistemi Windows e dei 10 bug che affliggono i sistemi UNIX. La lista, rintracciabile all'indirizzo www.sans.org/top20/, è stata messa a disposizione con lo scopo di **rendere note agli amministratori di tutto il mondo le informazioni che gli hacker hanno e sfruttano per penetrare nei sistemi**. L'FBI cambia così il proprio atteggiamento nei confronti della pirateria: da azione investigativa volta ad individuare ed eliminare i potenziali pericolosi ad azione preventiva degli stessi.

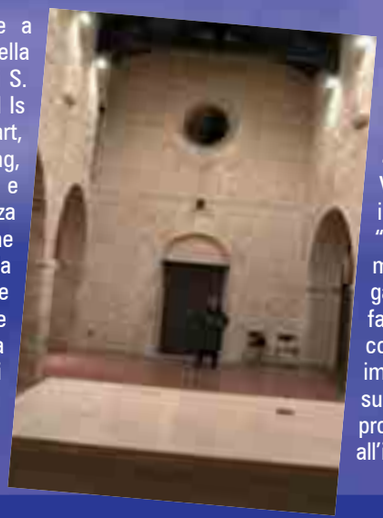


QUASI IL 50% DEL SOFTWARE È ILLEGALE!

Durante il convegno "La nuova legge sul diritto d'autore, un'opportunità per il mercato legale del software" tenutosi a Padova la BSA (Business Software Alliance) ha comunicato i risultati di una propria indagine effettuata nel nord-est del nostro paese. Questo è quanto viene detto dal vicepresidente della società Giovanni Ferrari: "Secondo lo studio condotto da Bsa **il tasso di applicazioni software privo di licenza utilizzati nelle aziende è del 45%**. Per il Triveneto poi, abbiamo dati ancora più allarmanti: le indagini condotte quest'anno dalla Guardia di Finanza hanno portato al sequestro di oltre 1800 prodotti software illegali per un valore di oltre 1 milione e 200 mila euro con **un tasso di illegalità aziendale del 75%**". Per concludere: "È chiaro che di fronte ad una situazione di questo genere all'attività di repressione e legalizzazione condotta dalle autorità competenti debba seguire un'intensa attività di informazione e collaborazione con il mercato".

D-I-N-A: DIGITAL-IS-NOT-ANALOG.2002

Dal 24 al 26 ottobre a Campobasso, nella chiesa sconsacrata di S. Bartolomeo, si terrà Digital Is Not Analog, festival di net.art, virus, media jamming, videogiochi modificati e hacking. Giunta alla terza edizione, la manifestazione ha come filo conduttore la rielaborazione di tecnologie e stili della comunicazione elettronica, e vede la partecipazioni di molti ospiti, tra cui spicca 0100101110101101.ORG, famoso per alcuni dei più famosi colpi mediatici degli ultimi anni, come la creazione e diffusione, all'inaugurazione della 49esima Biennale di Venezia, del virus informatico "biennale.py" o il memorabile furto della galleria d'arte Hell.com, un famoso sito d'arte, considerato quasi impenetrabile. Informazioni sugli altri ospiti e sul programma si possono trovare all'indirizzo d-i-n-a.net.



HACKBOOK

L'ETICA HACKER E LO SPIRITO DELL'ETÀ DELL'INFORMAZIONE

Autore: Pekka Himanem
Traduzione: Fabio Zucchella
Editore: Feltrinelli
Pagine: 175
Prezzo: 12.91

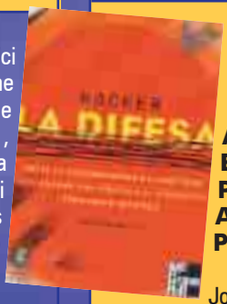
Un libro per spiegare che gli hacker non sono solo i creatori di virus o i ladri di dati come spesso ci viene raccontato. Sono soprattutto le persone che hanno permesso "la creazione del pc e del modem, l'affermazione planetaria di Internet, l'invenzione delle realtà virtuali." Cavallo di troia in Sendmail.

HACKER: L'ATTACCO

Autore: John Chirillo
Editore: Mc Graw HIll
Pagine: 933 (+ CD-rom)
Anno: 2002
Prezzo: 51.50

L'esperto di sicurezza John Chirillo ci guida in un viaggio "tecnogotico" nel mondo degli hacker illustrato da un hacker. L'autore ci insegna come scovare varchi nella sicurezza di un sistema e come capire quando siamo vittima di attacchi. Interessante è la parte di questo immenso volume, di quasi mille pagine, che viene dedicata al toolkit "Tiger Box" per insinuarsi nelle reti vulnerabili.

HACKER: LA DIFESA



Autore: John Chirillo
Editore: Mc Graw HIll
Pagine: 495 (+ CD-rom)
Anno: 2002
Prezzo: 29.50

John Chirillo, stesso autore di "Hacker:L'attacco", si concentra in questo volume sugli aspetti legati alla difesa di un sistema. Basandosi sulla sua esperienza di consulente presso numerose società, Chirillo descrive tutte le contromisure da attivare per la sicurezza dei propri sistema e dei daemon: si passa dai sistemi per impedire la raccolta di nostri dati sensibili fino alla rilevazione e protezione dalle backdoor.

HOT!

XBOX (DI NUOVO!) CRACCATA

Nelle scorse settimane, Microsoft aveva introdotto un nuovo tipo di protezione per la sua console X-Box. Queste protezioni dovrebbero servire a evitare l'esecuzione di software non autorizzati; oltre ai giochi copiati, questo comprende anche Linux (abbiamo spiegato come installarlo nello scorso numero). Diciamo che "dovrebbero impedire" perché **a neanche una settimana dall'introduzione della nuova protezione, questa è già stata craccata da due diversi utenti**. Il bello è che non c'è nemmeno bisogno di modificare l'hardware della macchina. Per ora, Linux su X-Box può continuare a girare tranquillo.

NUOVO RECORD DI ELOCITÀ

Durante un convegno xx, due ricercatori dell'Università dell'Illinois hanno raggiunto la **velocità record di 2,8 Gigabit al secondo su una dorsale transoceanica**, che congiunge USA ed Europa.
La nuova tecnica, chiamata Photonic Data Services (PDS) è in grado di trasmettere dati a una velocità di circa 500 volte superiore a quella raggiungibile oggi con i protocolli standard di Internet. Con tanta banda a disposizione, chissà come funziona WinMX... ;-)

NON PAGARE QUESTA MUSICA!

Questo è il coraggioso slogan di Anomolo, un'etichetta musicale indipendente italiana che non solo distribuisce la musica prodotta gratuitamente su Internet, ma non pone nemmeno alcun limite alla sua circolazione. **Tutti i brani scaricabili sono infatti liberi da copyright e non registrati presso la SIAE**. Per cominciare a scaricare musica davvero libera, basta puntare il proprio browser all'indirizzo www.anomolo.com

"LA SICUREZZA È UN PROCESSO, NON UN PRODOTTO"

>Bruce Schneier

CIFRATURA A 64BIT SUPERATA

La condivisione delle risorse, è questa l'arma utilizzata da **distributed.net, che ha coordinato il lavoro di oltre 330.000 computer.** Una potenza di calcolo enorme, che è riuscita ad elaborare la bellezza di 15.769.938.165.

961.326.592 combinazioni prima di individuare la chiave corretta per superare "RC5-64 Secret-Key Challenge" della RSA security che aveva lanciato la sfida qualche anno fa. Distributed.net oltre a ricevere gli elogi si appresta a ricevere un assegno di diecimila dollari dalla RSA come ricompensa.

PREZZI DEI CD MUSICALI TROPPO ALTI? FORSE ABBIAMO RAGIONE

Che i CD musicali fossero troppo costosi è opinione diffusa, ma ci siamo sempre sforzati di credere alle parole delle case di produzione che continuano a dirci che i costi elevati sono dovuti agli investimenti molto alti per la ricerca di nuovi artisti, alla realizzazione del supporto, alla promozione pubblicitaria….
Warner, Sony Music, Universal Music, EMI Music e Berteslmann Music **dovranno versare ben 67.3 milioni di dollari di multa per aver mantenuto i prezzi dei CD troppo alti**.

Questa è la somma che le case discografiche hanno deciso di versare per mettere fine ad una delicata causa antitrust che da molti mesi li vedeva sotto inchiesta: oltre 120 miliardi di vecchie lire per non dover ammettere di aver creato un cartello dei prezzi. Insomma, come dire, vi diamo questi soldi, ma basta che ci lasciate continuare. Inutile dire che gli acquirentri non potranno in alcun modo ricevere nemmeno una fettina di questa ingnete somma. Come al solito, cornuti e mazziati.

"POLICEWARE" MADE IN USA

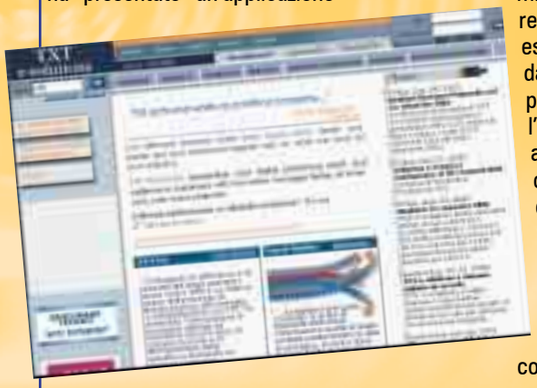
Rendere obbligatorio l'inserimento di tutti gli strumenti tecnologici possibili come strumento antipirateria: è questo il tema in discussione in questi giorni negli Stati Uniti d'America.
La Consumer Broadband and Digital Television Promotion Act (CBDTPA, la legge in discussione) è molto criticata in quanto **permetterebbe di inserire degli spyware, ribattezzati per l'occasione policeware, che minerebbero sicuramente la privacy degli utenti**. Tecnologie hardware e software volte a permettere un rapido accesso negli apparecchi come **personal computer o televisioni per garantire le proprietà intellettuali e la sicurezza del paese**: ancora una volta, ci si chiede di barattare una presunta maggiore sicurezza, con una certa rinuncia del fondamentale diritto alla privacy.

LA MACCHINA DELLA VERITÀ NON DICE LA VERITÀ!

È quanto affermato dal National Research Council. L'NRC ha affermato che l'alto grado di errore delle tecniche poligrafiche **rende il sistema inaffidabile e per questo non utilizzabile**. L'FBI, che da tempo utilizza le macchine della verità per alcune indagini, si trova ora con l'emergenza di trovare un metodo alternativo, anche se a dire il vero questo è ben lungi dal venire. Frank Horvath, noto docente di criminologia, contesta comunque questa tesi, affermando che "l'assenza di una alternativa, rende di fatto inevitabile l'uso della macchina della verità".

FIREWALL P3P

TXT e-solution (www.txt.it), in collaborazione con il centro di ricerca dell'Unione Europea Joint Research Centre, ha presentato un'applicazione completa dello standard P3P (Platform for Privacy Preferences), standard studiato dal World Wide Web Consortium sin dal 1997 per migliorare la gestione dei dati personali sulla rete. L'applicativo, che è open source, essendo realizzato in Java è indipendente dalla piattaforma utilizzata. Il sistema P3P prevede una collaborazione tra il sito e l'utente: quando le specifiche P3P saranno accolte da entrambi i lati della comunicazione sarà possibile per l'utente conoscere, in modo preciso, i tipi di dati che vengono recuperati dal sito e le finalità degli stessi. Quindi piena libertà dell'utente che attraverso il meccanismo delle autorizzazioni potrà consentire lo scambio solo dei dati essenziali o impedirlo completamente.



IL WORM SLAPPER CONTINUA AD EVOLVERSI

I computer worm in poco tempo si sono molto diffusi e non poteva che essere così anche per Slapper, un worm che ha preso di mira i server Linux. **Dopo aver infettato oltre 20.000 server nella sua versione originale, Slapper si è evoluto in almeno 5 varianti, continuando così la sua diffusione**.
L'ultima variante che si è diffusa su internet è Mighty, piccola evoluzione del già diffuso DevNull.
Mentre tutte le versioni precedenti a DevNull creavano una rete peer-to-peer per comunicare tra loro, quest'ultimo utilizza una chat per poter comunicare con il proprio creatore. Si ritiene comunque che le tecniche che hanno sfruttato la vulnerabilità SSL si esauriranno in fretta in quanto la maggioranza degli amministratori è ormai a conoscenza del problema ed ha già provveduto a risolverlo.

FALLE E BACHI

Microsoft ha divulgato tre problemi di sicurezza per gli sviluppatori che usano le librerie RPC sui Services for Unix 3.0 Interix SDK. il link al bollettino è
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-057.asp

Problemi di sicurezza sono stati individuati in un controllo Activex presente nel sistema di help di Windows. Le versioni colpite sono Windows 98 SE, Millenium Editino, NT 4.0 e Windows Xp. I problemi sono due: il primo è basato su un buffer non verificato e permette l'esecuzione di codice arbitrario. Il secondo buco è basato sui file di estensione .chm che in particolari condizioni questi possono permettere l'esecuzione di azioni arbitrarie e senza controllo sul sistema locale. Il bollettino ufficiale:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-055.asp

All'indirizzo
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-056.asp
Microsoft mette a disposizione un kit di pach cumulative per risolvere le vecchie e le nuove vulnerabilità che riguardano SQL Server 7.0, SQL Server 2000, Microsoft Data Engine (MSDE) 1.0, Microsoft Desktop Engine (MSDE) 2000.

HJ ha surfato per voi...

http://www.dvara.net/HK

HK sta per Hacker Kulture. Lo definisco il sito della cultura hacker, una sorta di grandiosa e imponente biblioteca virtuale dedicata alla storia, alla filosofia, all'etica e persino alla poesia e all'arte hacker! Per sua stessa natura, il sito è in perenne costruzione. Insomma va aggiornato di continuo e per ora siamo solo in due. Ciò che voglio far capire attraverso HK è che la tecnica sì è importante perchè ti permette di esprimere al meglio le tue idee...ma le idee non le acquisisci tramite le tecniche! La rete pullula di tecniche...credo che sia giunta l'ora di ripercorrere, soprattutto di questi tempi,
anche un pò l'ideologia hacker, il fine dell'hacking, lo spirito hacker. Steven Lévy scrive:
" L'hacker...[pratica]...l'esplorazione intellettuale a ruota libera delle più alte e profonde potenzialità dei sistemi di computer, o la decisione di rendere l'accesso alle informazioni quanto più libera e aperta possibile. Ciò implica la sentita convinzione che nei computer si possa ritrovare la bellezza, che la forma estetica di un programma perfetto possa liberare mente e spirito".
Se conosci solo la tecnica puoi cambiare un sistema informatico; se sei anche ideologicamente un hacker allora puoi anche cambiare il mondo...o comunque tentarci! In ogni caso migliori te stesso!!! L'accesso a tutte le informazioni è bene, purchè non ne venga esclusa nessuna! Stringere con forza nel palmo della propria mano tutto il sapere è bene, purchè questo non ti faccia sentire egoisticamente potente! Il rischio c'è, ora più che mai, di stravolgere ciò che si è acquisito, tecnicamente parlando, per metterlo al servizio del proprio ego o peggio ancora di un sistema ingiusto. Ed ecco quindi la necessità di "non dimenticare"; la necessità di "ricordare"!
Non è la tecnica che fa di te un "hacker", ma la "forma mentis" e l'etica! Prorpio E.S. Raymond, affrontando la questione dell'etica hacker, ha scritto:
"Gli Hackers risolvono i problemi e costruiscono le cose, credono nella libertà e nel mutuo aiuto volontario. Per essere accettato come un hacker, ti devi comportare come se avessi questo atteggiamento nel sangue. E per comportarti come se avessi questo atteggiamento nel sangue, devi realmente credere nel tuo comportamento. Se pensi a coltivare un atteggiamento da hacker giusto per essere accettato
nella hacker-culture, allora non hai capito. Diventare il tipo di persona che crede in queste cose è importante per te per aiutarti ad imparare e per avere delle motivazioni. Come con tutte le arti creative, la via più efficace per diventere un maestro è imitare la forma mentis dei maestri - non solo intellettualmente ma anche emotivamente."

15 minuti di celebrità! Questi sono i

http://www.ubrihackers.it

Sono il fondatore della ubrihackers crew. Chiedo cortesemente che il nostro sito sia segnalato su HJ.

Perfidix

www.hacker-school.com

Questo portale si occupa di sicurezza informatica e di tutto quello che per noi è l'hacking, nella forma più etica possibile.

Rspide

Segnalate i vostri siti a: redazione@hackerjournal.it

vostri siti; scegliete voi se tirarvela o vergognarvi

http://digilander.iol.it/rpl/

Se volete info e materiale per hacking o programmazione, siete i benvenuti! Ciao.

MaxTheGreat

www.gxware.bgo.net

Mi chiamo gloxX e gestisco insieme a miei due amiciun sito che si occupa principalmente di masterizzazione e Linux. È è dal 6 numero che vi seguo (e non ne perdo nemmeno uno) ma ho tutti i pdf e gli sfondi degli arretrati!!! P.S. Leggo tutto il vostro giornale in circa 15 minuti...vi sembro troppo "assatanato"??? :)

gloxX

www.alexbessi.com

Bravi! Complimenti per il lavoro svolto fino ad ora, nonostante le critiche (giuste) sui primi numeri siete riusciti a continuare migliorando, è cosi' che si fa! Colgo l'occasione per segnalare il mio sito: www.alexbessi.com che si occupa di Linux, programmazione, security e linguaggi web. A proposito troverete tante guide, manuali e tutorial! inoltre è possibile inviare il proprio sorgente e vederlo pubblicato nell'apposita sezione del sito!

Alex

www.atstake.com

Oggi le aziende tendono ad assumere degli hacker come esperti di sicurezza (e non a torto: chi può difenderli meglio?). Qualche anno fa però le cose non stavano così, e la notizia della fusione tra @stake (azienda di security) e gli hacker di L0pht Heavy Industries aveva creato un certo scalpore. Sul sito di @stake si possono trovare notizie interessanti, viste con l'occhio di chi si occupa di sicurezza, ma è stato dall'altra parte della barricata.

Il Grande Fratello si chiama Palladium

Altro che Orwell: se il progetto Palladium di Microsoft andrà in porto, saremo tutti un po' meno liberi e un po' più spiati.

COS'È, COME FUNZIONA E QUALI GUAI PRODURRÀ PALLADIUM

È inutile nascondercelo, stiamo vivendo un periodo molto difficile. I fatti dell'11 settembre 2001 hanno cambiato molte cose nel mondo che ci circonda e soprattutto hanno portato alla luce un aspetto del problema che prima preferivamo ignorare o, peggio ancora delegare in toto a qualcun altro: la sicurezza.
Prendendo la palla al balzo, in modo esplicito negli USA e di riflesso in Europa, i politici ci hanno messo di fronte ad un a scelta: **barattare la nostra privacy in cambio di una maggiore sicurezza.**
Purtroppo sotto l'onda emozionale ed una spinta dei media, molte persone hanno risposto positivamente a questa richiesta, anche se il problema era completamente sbagliato e la sicurezza poteva essere ottenuta anche nel rispetto della privacy e dei diritti costituzionali. La storia ci insegna, tristemente, quanto sia importante per il potere politico aumentare il controllo sulla popolazione, visto che da questo dipende il proprio futuro. C'è quindi qualcuno che ha visto in questo un business e ha tirato fuori dal cas

setto i piani già pronti per un "computer sicuro" e li ha mostrati a tutti.
Il consorzio TCPA (Trusted Computing Platform Alliance) ha le sue radici nel lontano ottobre 1999, quando Compaq, HP, IBM, Intel e Microsoft hanno messo le radici per **"un'iniziativa focalizzata nel migliorare la fiducia e la sicurezza nei computer"**. Ora questa alleanza ha piu' di 150 partecipanti.

Il sito della TCPA, Trusted Computer Platform Alliance, principali promotori di Palladium (www.trustedcomputing.org).

>> Ecce Palladium

Palladium è un'architettura hadrware e software che permette di controllare tutte le applicazioni che funzionano all'interno del PC , a partire dal disco di boot, in modo molto simile al sistema di "blindatura" della console X-Box.
In un computer Palladium, già al momento del boot viene verificato il contenuto della flash rom responsabile del boot e la chiave di accesso al disco, che è cifrato (magari scritta al suo interno direttamente dal produttore), per verificare che il supporto sia omologato ed adatto allo standard di sicurezza. Effettuata questa verifica, il sistema può decifrare il disco e caricare "regolarmente" il kernel del sistema operativo. In fase di boot vengono anche state verificate tutte le connessioni con le periferiche, come la tastiera, visto che solo le periferiche che sono riconosciute dal sistema grazie alle loro chiavi potranno essere abilitate. La stessa tastiera comunica con il sistema attraverso un

canale cifrato, per evitare che possa essere facilmente decifrata da qualche programma residente.
Il cuore del sistema è il componente di cifratura, che a seconda delle diverse fonti di informazione può essere inserito all'interno della CPU come set di funzioni estese (AMD per esempio) oppure come chip a se stante che si frappone tra la CPU ed il resto della motherboard a cavallo del south bridge (che controlla il bus PCI).
Palladium gestisce tutti i processi del PC. **Prima di avviare un processo, questo viene sottoposto all'attenzione del sistema di controllo, che ne verifica le credenziali (la chiave) e l'integrità.** Ma non solo! Ogni singolo file che viene mostrato, immagazzinato o trasmesso viene sottoposto allo stesso esame.
Di conseguenza **è possibile che un messaggio di posta che avevamo immagazzinato per promemoria, svanisca** perché chi lo ha spedito vi ha impresso sopra una data di scadenza, oppure che **quando riproduciamo un file Mp3 il sistema di DRM (Digital Rights Management) ci chieda di dimostrare che abbiamo anche il CD originale** prima di eseguire il brano (a questo punto può anche cancellarlo o acquistarne i diritti in modo automatico/autonomo come il produttore del player ha deciso si debba comportare)
Mario Juarez, product manager per la unità di "content security business" in Microsoft, sostiene che "Palladium non è il DRM, ma è solo la piattaforma ideale per costruirci sopra un gestore di DRM", come dire che se non è zuppa è pan bagnato.

>> Sicurezza e rischi

Ancora non è dato sapere nulla sulle specifiche tecniche dettagliate dell'architettura hw/sw di Palladium, ma è certo che Palladium sarà comunque basato su un cuore che gestisce la cifratura dei dati, e l'accesso a questo tramite delle chiavi di lunghezza (e quindi sicurezza) piuttosto elevata. Come in tutti i sistemi di cifratura, il cuore del problema è la reale sicurezza dei dati e i dubbi che sorgono sono relativi a tre punti chiave:
- gli algoritmi usati;
- la cifratura di tutte le comunicazioni tra il PC ed il gestore delle risorse (e quindi non è possibile sapere quali dati vengono inviati ai gestori su internet dal nostro sistema);
- l'eventuale presenza di una backdoor (o Master Key) che permette a Microsoft o a un qualche governo di aprire tutti i file del sistema e di conseguenza le garanzie di custodia/furto della chiave stessa.
Gli algoritmi di cifratura sono il prodotto di sofisticati e robusti sistemi matematici, non il risultato di una brillante intuizione. Gli algoritmi devono essere valutati dalla comunità perché potrebbero avere un tallone di Achille che li rende facili preda di un programmatore smaliziato, magari più brillante dello scienziato che ha inventato l'algoritmo. In pratica, non è necessari reinventare l'acqua calda quando sono a disposizione decine di algoritmi di cifra-

Link utili

Le Faq su Palladium in Italiano
www.complessita.it/tcpa

Gates e la Cina
www.cw.com.hk/Comment/c990713001.htm

InfoWorld: Microsoft serves up Palladium details
www.infoworld.com/articles/hn/xml/02/07/29/020729hnpalladium.xml

VeriSign issues false Microsoft digital certificates:
www.itworld.com/Sec/4039/IW010322hnmicroversign/

Microsoft to reveal Palladium source code:
http://news.com.com/2100-1001-938973.html

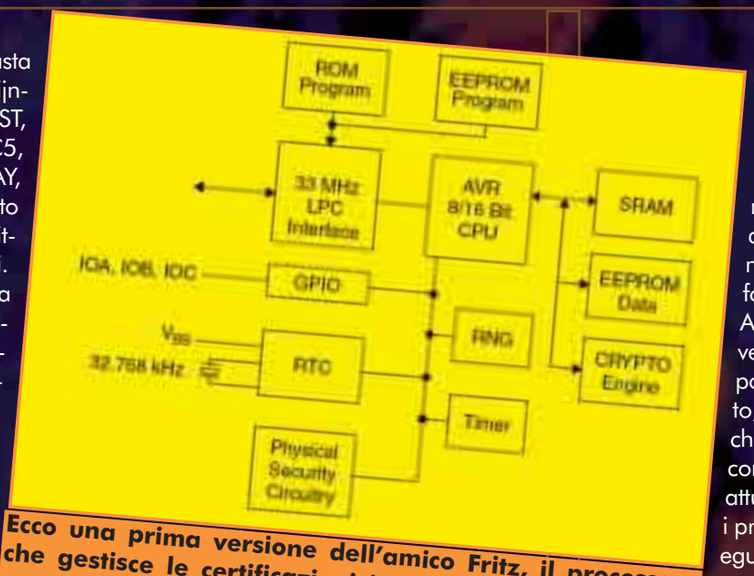
The Big Secret
http://cryptome.org/palladium-sl.htm

10 cose che non faremo più

Ok, stiamo tirando un po' a indovinare, ma abbiamo voluto provare a immaginare quali conseguenze il nuovo sistema di Microsoft potrebbe avere sulle attività quotidiane di ognuno di noi. Ecco una lista:

1 Rippare CD e DVD
Le connessioni tra lettore e Cpu sarebbero cifrate, e non sarebbe possibile intercettare questi dati.
2 Scaricare, eseguire o duplicare formati di file non protetti (Mp3, Mpg, Wav, Aiff).
Il sistema di Digital Right Management potrebbe limitare l'utilizzo di tutti i formati che non utilizzano un sistema di autenticazione dei contenuti.
3 Usare un keylogger
Anche i dati in arrivo dalla tastiera dovrebbero essere cifrati, per cui non possono essere intercettati.
4 Usare driver non ufficiali per le periferiche, o periferiche non supportate
Il sistema può rifiutarsi di far funzionare una periferica con un driver alternativo (come quelli di www.kxproject.com per le schede audio).
5 Usare software alternativo
Il formato di file dei documenti potrebbe essere sottoposto alle regole restrittive per la gestione del contenuto. Open Office, che cerca di utilizzare formati di file proprietari, potrebbe quindi diventare illegale.
6 Eseguire un backup del software o di contenuti multimediali
Ancora una volta, i meccanismi di controllo del copyright potrebbero impedire operazioni perfettamente lecite, come l'esecuzione di una copia di backup personale.
7 Usare freeware e software a basso costo
Ottenere una chiave per firmare i propri software potrebbe avere un costo che renderà impossibile la realizzazione di freeware. La chiave di un software non potrà essere divulgata, e quindi non potranno essere pubblicati i sorgenti del programma. Questo impedirebbe l'utilizzo di software open source per Windows.
8 Vedere film o ascoltare musica su sistemi non Palladium compatibili
Le majors potrebbero produrre CD e DVD che possono essere riprodotti solo su sistemi Palladium, tagliando fuori tutti gli altri.
9 Vedere alcuni siti Internet
Siccome i loro certificati non saranno conformi a quelli della nostra macchina, verranno automaticamente oscurati perché potenzialmente pericolosi.
10 Non potreno piu fare scherzi agli amici
Tutti i siti, anche quelli dove non siamo mai stati, ci diranno all'arivo: "Benvento dott. Gugielmo, come sta? E la famiglia? Ho visto che una ora fa sua moglie ha comprato un'aspirina su www.compramedicinali.it...

tura stabili ed approvati da una vasta comunità internazionale. (AES/Rijndael, RC6, MARS, Twofish, CAST, IDEA, DES, Triple DES RC2, RC5, Blowfish, Diamond2, TEA, 3-WAY, GOST, CAST). Palladium, in questo caso, dovrebbe usare degli algoritmi di cifratura pubblici e certificati. Per quanto riguarda la custodia delle chiavi, il problema non è facilmente risolvibile, basta guardare ad un paio di episodi poco edificanti successi nel cosso dell'ultimo anno. Il 29 ed il 30 gennaio 2001 **VeriSign ha emesso per errore due certificati Microsoft a un impostore mettendo in serio pericolo gli utenti.** Mahi De Silva, vice presidente di VeriSign, ha comunicato che questi sono gli unici due certificati fraudolenti emessi per errore, tra gli oltre 500.000 certificati enessi dalla società di garanzia, ha inoltre specificato che prima dell'emissione (la richiesta avviene in modo elettronico) due persone controllano e verificano i dati manualmente. Un altro esempio e quello che è successo con i Dvd ed il programma DeCSS quando il castello delle chiavi e dei certificati è stato compromesso dalla fuga di notizie (per i DVD un errore della Xing che ha divulgato la propria chiave di encription grazie al riverse engineering del suo player ad opera di MoRE (Masters of Reverse Engineering).



Ecco una prima versione dell'amico Fritz, il processore che gestisce le certificazioni in Palladium. Il nome del processore è stato ispirato da un senatore americano che ha spinto per l'introduzione del TCPA.

>>Open source: la risposta

L'unica soluzione a tutti questi dubbi è quella dell'Open source. Solo permettendo agli utenti di verificare il codice, e soprattutto di poterlo successivamente ricompilare per verificarne l'effettiva integrità, è infatti possibile garantire gli utenti contro la presenza di errori grossolani e sottili, ma anche fugare ogni dubbio sulla presenza di trappole e sotterfugi. Un esempio di questa politica e quella seguita per PGP, che sviluppato da Philip Zimmermann con sorgenti pubblici, ha raccolto un enorme successo fino all'acquisto di NAI, con un blocco della diffusione per il timore che la grande società avesse potuto immettervi delle chiavi "speciali" (Master Key, in gergo) di controllo sotto la pressione del governo americano. NAI è stata quindi costretta a vendere nuovamente PGP a una società privata (Pgp Corp, www.pgp.com) che continuerà proporre il prodotto in open source.

Durante il processo dell'antitrust a Microsoft, Jim Allchin, senior vice president per Windows, ha sostenuto "Più cose i creatori di virus conoscono sui meccanismi di protezione del sistema operativo, più facile diventa per loro creare virus che possono disabilitare questi meccanismi", a sostegno dei pericoli intrinsecamente legati alla piattaforma Open Source.

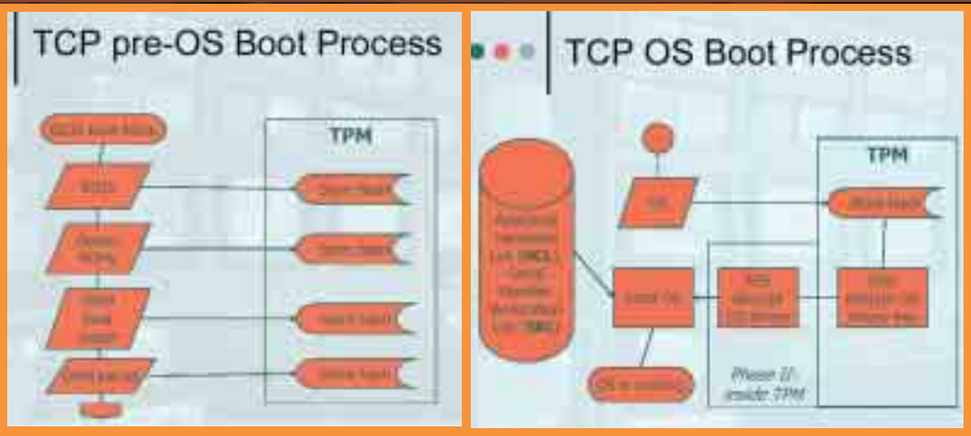
A sorpresa Juarez ha invece detto che il codice potrebbe essere pubblicato, questo non significa che sarà Open Source, a conferma di una teoria più attuale che dimostra come i progetti open source siano egualmente sicuri rispetto a quelli "protetti".

Molto sorpreso, ma anche soddisfatto dalle affermazio-

Un legittimo sospetto

Gli analisti che hanno qualche dubbio sul sistema Palladium sono. Anni di insuccessi nel campo della sicurezza e un fondamentale atteggiamento di indifferenza verso le segnalazioni di problemi degli utenti (il tutto mascherato da comunicati stampa trionfali sulla sconfitta di virus e trojan horse), hanno portato una fascia del pubblico a odiare il colosso di Redmond, come se stesse combattendo una guerra santa, altri a dubitare sempre delle parole di Bill Gates, una ulteriore parte ad avere un atteggiamento molto freddo verso le promesse della software house.

Anche se alcuni dati lasciano pensare che poi dopo tutto Windows 2000 non sia peggio degli altri sistemi operativi: in un articolo del 24 settembre 2001 e basato sulle segnalazioni di Bugtraq, John McCormick evidenziava, che le falle segnalate erano in numero assolutamente comparabile a quelle degli altri sistemi operativi, suscitando un vespaio di polemiche e popolando con le sue affermazioni le slide promozionali della Microsoft (notate che i problemi di W2K sono contati separati da quelli di IIS, sommando i due Windows balza immediatamente in testa alla classifica del disonore).



Lo schema delle verifiche effettuate al boot, tratto dalla presentazione che Lucky Green ha tenuto al DefCon X (la presentazione si trova in formato Pdf e PowerPoint su www.cypherpunks.to).

ni di Juarez, è Bruce Perens, un evangelista del progetto e creatore della stessa definizione di Open Source: "Penso che Microsoft stia ammettendo che può diffondere il codice sorgente a tutto il mondo, senza necessariamente urtare la sicurezza dei programmi"

>>Distribuzione delle chiavi

Ultimo dei problemi è senza dubbio la distribuzione delle chiavi. Chiunque sviluppi un software o un sistema operativo, senza acquistare una chiave non potrebbe distribuire il suo prodotto. Altresì ci sarebbe una commissione che dovrebbe valutare l'applicazione per vedere se contiene backdoor oppure del codice malizioso. Tutto questo fa sì che **il costo di una chiave possa lievitare a valori che un produttore amatoriale di software non si può permettere.**

I notebook ThinkPad della serie T di Ibm sono tra i primi computer a incorporare i circuiti per la gestione delle restrizioni TCPA.

Inoltre chi giudica se un programma è sicuro? Magari scopriamo che un sistema per rippare i CD viene giudicato "non sicuro", alla faccia del diritto di backup, e quindi non gli viene data la chiave.
Nelle mani di chi volgiamo mettere la scelta di quali software possono essere installati ed utilizzati sul nostro PC?

>>Ma quando arriva?

Il progetto Palladium dovrebbe vedere la luce nel 2004 anche se si pensa che l'architettura potrebbe essere completamente implementata e acquista dal mercato verso il 2006.
Nel frattempo è di grande interesse vedere cosa si muove riguardo le misure anti pirateria e DRM sulla piattaforma Microsoft, con l'introduzione del nuovo Media Player 9 ma già presente nella versione 7, con la lettura del licence agreement che recita (tradotto dall'inglese)
"Voi accettate che per poter proteggere l'integrità del contenuto e del software protetto dal DRM, Microsoft può fornire aggiornamenti di sicurezza ai componenti del sistema operativo, che potranno essere scaricati (ed installati) automaticamente sul vostro Computer. Questi aggiornamenti di sicurezza potranno disabilitare la possibilità di copiare o mostrare i file con "Contenuto Sicuro" o l'uso di altri software all'interno del vostro computer".
Secondo qualcuno però, Palladium diventerà davvero una realtà **quando Microsoft deciderà davvero di porre un freno alla pirateria software, fin qui tutto sommato tollerata**, per mostrare il conto a chi usa programmi copiati. Bill Gates ha sognato per anni di trovare un modo di fare pagare il software ai Cinesi, Palladium potrebbe essere la risposta alle sue preghiere: ecco cosa ha detto Gates agli studenti dell'università' di Washington nel lontano luglio 1999: "Nonostante in Cina vengano venduti circa tre milioni di computer ogni anno, le persone non pagano per il software. Un giorno, comunque, lo faranno. Fintanto che lo rubano, noi vogliamo che rubino il nostro. Ci si abitueranno e dopo, in qualche modo, troveremo come riprendere il denaro, prima o poi nel prossimo decennio"
Infine, una nota storica. Trovo molto divertente e sottilmente ironico è il nome del prodotto, Palladium, preso in prestito dalla mitologia greca, dato che Palladio è il nome del gigante ucciso dalla dea Atena, dea della guerra, della saggezza e delle arti liberali, ma anche protettrice della città di Troia, e tutti sappiamo che **fu espugnata da Ulisse grazie allo stratagemma del Cavallo di Troia**, appunto. Che in questo ci sia un "involontario" messaggio di ammonimento? A buon intenditore, poche parole.

Guglielmo Cancelli

(Guglielmo.Cancelli@hackerjournal.it)

COME METTERE IN REGOLA IL SOFTWARE ACQUISTATO IN ALTRI PAESI

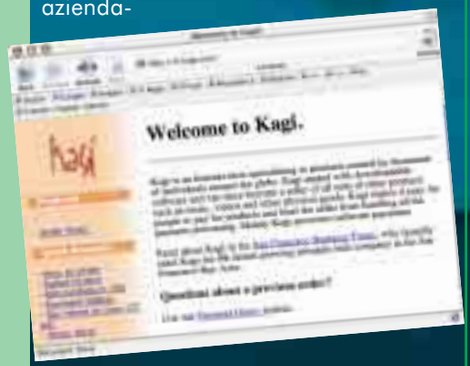
Comprare all'estero

Per la Finanza, la prova più convincente della "regolarità" del software è la fattura; ma come fare quando il progrmama è stato acquistato e scaricato via Internet?

Soprattutto in ambito aziendale vi sono molti dubbi su come acquistare software Shareware o dall'estero e come poterlo poi regolarmente mettere in contabilità aziendale. Lasciando perdere quanto relativo alla bollinatura SIAE - per maggiori informazioni conviene rivlgersi direttamente alla SIAE anche se in alcuni casi non è previsto il bollino per il software - si può sintetizzare la legge in tutela del software questa prevede sanzioni per chi duplica o utilizza programmi per elaboratore senza averne diritto. Il diritto all'uso del programma, dipendendo dall'acquisto della relativa licenza d'uso, viene acquisito all'atto dell'acquisto e pertanto si è perfettamente in regola sotto questo punto di vista.

>>"Scaricare" i programmi scaricati

Innanzitutto occorre fare una distinzione tra il software "pacchettizzato" - ovvero costituito da confezione, manuali CD e altro - e il software che invece viene acquistato e prelevato dai server (download) solo in forma elettronica.
Per quanto riguarda il software acquistato onLine (o la shareware che viene registrato all'estero) il suo uso anche in ambito azienda-



le è regolarissimo. **La cosa leggermente più complessa è la registrazione della fattura da richiedersi sempre al venditore**. Per registrarla è infatti necessario una autofattura in cui si farà riferimento alla fattura originale del fornitore, si indicherà qual'è il bene acquistato e quale sia il suo prezzo, espresso in valuta italiana. Per la determinazione del prezzo in valuta italiana, è comodo allegare all'autofattura la copia dell'estratto conto della carta di credito usata per il pagamento oppure, in caso di trasferimento tramite banca (raro e caro), si allegherà la documentazione bancaria con indicato **l'importo in Euro. Su questa autofattura verrà applicata anche l'IVA, che potrà poi essere dedotta a livello contabile** essendo questa sia una fattura di vendita che al tempo stesso di acquisto.

>>Pacchi e spedizioni

Per il software costituito anche da beni materiali (supporti dati, confezioni, manuali eccetera), essendoci il transito di questi da una dogana, è necessario anche pagare il relativo Dazio oltre all'IVA. Se si chiede al fornitore di spedire il materiale tramite un corriere internazionali (per es. Federal Express), **sarà quest'ultimo ad effettuare tutte le pratiche di sdoganamento** e ad anticipare (per piccoli importi) IVA e Dazio. Unitamente alla merce si riceverà poi dal corriere una "fattura doganale" che potrà essere messa in contabilità.
Ultimo caso in esame, è quello dei prodotti acquistati di persona all'estero e poi importati in Italia. In questo caso è consigliabile contattare uno spedizioniere prima della partenza - è facile trovarne in quasi tutti gli aeroporti - e chiedergli tutte le informazioni del caso. Fino a un po' di anni fa, rivolgendosi a uno spedizioniere la prassi era decisamente semplice. Era infatti sufficiente compilare una distinta dei beni da sdoganare e condegnarla, unitamente al materiale, allo spedizioniere. **Come nel caso del corriere inernazionale, anche lo spedizioniere consegnerà una fattura doganale da mettere in contabilità.**

>>Risparmiare qualcosa

In tutti i casi di importazione fisica di un prodotto software, se il software è venduto disgiunto dai manuali o se sono voci distinte in fattura, è consigliabile indicare ogni voce per conto proprio con il relativo prezzo. Il motivo di ciò è presto detto: **le aliquote possono essere diverse a seconda del fatto che si tratti di un programma oppure di un manuale (di norma equiparato ai libri e quindi con imposte più basse).**
Queste pratiche di importazione diretta non sono sempre convenienti dato che la maggior parte dei software sono disponibili anche in Italia. Nel cso però di necessità di prodotti particolari o non distribuiti in Italia, l'importazione è decisamente un'operazione semplice soprattutto visto che ci si avvale normalmente di corrieri o spedizionieri che forniscono un servizio molto comodo.

ENZO BORRI

LE TIPICHE TECNICHE DI ATTACCO SU IRC

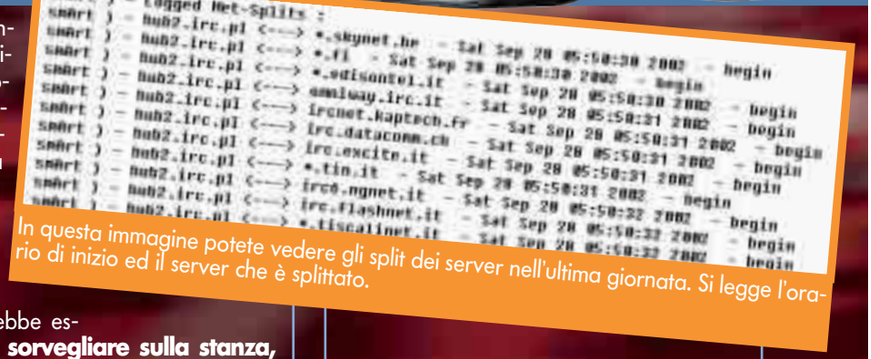
IRCWAR E SICUREZZA IN IRC

Tra gli utenti Irc a volte si scatenano delle vere e proprie guerre per la supremazia su un canale, o semplicemente per vandalismo. Ecco quali sono le armi utilizzate e i metodi per contrastarle.

Quanti di voi frequentano canali che la sera quando andate a dormire "vanno a dormire" insieme a voi? Direi nessuno lo stesso sono un gestore di più canali ed il mio scopo è far in modo che essi siano sempre attivi, sempre presenti e sempre utilizzabili da chiunque ci voglia chattare all'interno. Ma come disse un noto personaggio della politica "il potere logora che non ce l'ha" e proprio a causa di ciò, o meglio, proprio per la voglia di ottenere potere e, tradotto nei nostri termini, di gestire canali, è stato inventato **l'IRCwar, insieme di tecniche utilizzate per "rubare" stanze o sconnettere utenti.**
Spero di riuscire, in questa brevissima guida, a dare qualche suggerimento agli operatori sul come difendersi da tali attacchi, spiegandone il principio di funzionamento.

>> L'importanza di essere OP

Gli OP, o meglio ancora gli operatori del canale, sono coloro che detengono il "potere" all'interno del canale stesso. Hanno possibilità di estromettere utenti, di non permettere loro l'ingresso, di configurare le impostazioni del canale stesso; sono in pratica la nuvoletta nera che può fare il bello ed il cattivo tempo. Il loro compito dovrebbe essere quello di **sorvegliare sulla stanza, sovrintendendo all'attività e non agendo da sceriffi solo perché hanno possibilità di farlo**. Cose dette e ridette, solo per introdurre un concetto fondamentale: lo scopo primario dell'IRCwar nel caso qualcuno cerchi di takkare un chan inizia proprio dal cercare di assumere lo stato di OP. Come si riesce a fare ciò? Ah beh largo spazio alla vostra fantasia! Se individuate un metodo infallibile comunicatemelo, ve ne sarò grato! Di certo il social engineering è uno dei metodi più utilizzati. È basato su due principi cardine: il tempo e la vostra "simpatia". Unendole potrete riuscire pian piano ad entrare nelle grazie di qualche OP di botnet che magari vi adderà sui propri BOT. Una volta raggiunto questo privilegio sarà un gioco da ragazzi in un momento in cui il chan è vuoto di altri operatori deoppare tutti e restare l'unico proprietario! Un po' da stronzi, ma efficace!



In questa immagine potete vedere gli split dei server nell'ultima giornata. Si legge l'orario di inizio ed il server che è splittato.

BOT: client IRC che girano su shell in maniera del tutto autonoma e continuativa nel tempo. I loro proprietari possono configurarli in modo da far compiere loro azioni ripetitive ed azioni di difesa.

>> L'artiglieria pesante

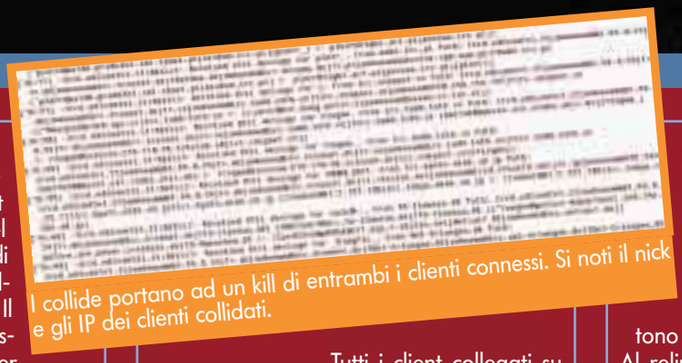
Un altro metodo utilizzabile si basa sul **mass-nuking; è un tipo di attacco "vecchia maniera" perché può avere significato solo su canali popolati da**

una cerchia assai ristretta di utenti. Il suo scopo sta nel forzare la disconnessione di tutti i client presenti e rientrare per primo nel canale acquisendo così lo status di OP. La tecnica utilizzata si basa sull'uso di nuke, di flood, o di smurf. Il nuke ha come principio l'invio massiccio di dati ad un PC. Il computer remoto, nelle vecchie versioni di windows, ha un bug di sistema per cui non sa gestire una tale mole di dati non richiesti che arrivano improvvisamente e si blocca. Risultato, l'utente deve riavviare il PC sconnettendosi quindi dal canale. **Il flood è una metodologia simile che si basa anch'essa sull'invio di grandi quantità dati** al PC remoto. Il modem non sopporta il carico e sospende la connessione. Se proprio avete due minuti da perdere provate a fare /list 0 (zero) e capirete di cosa sto parlando. Come potete ben capire, questi attacchi sono validi più in teoria che in pratica, anche per la ragione che normalmente quando avete finito di attaccare l'ultimo utente il primo avrà già riavviato il computer e sarà entrato di nuovo nel canale. Lo smurf è un attacco indiretto, nel senso che usa una terza via per arrivare all'IP da colpire. Con l'utilizzo di indirizzi broadcast che amplificano la mole di dati inviata e il successivo reindirizzamento all'utente finale, questo viene raggiunto da migliaia di Kb che lo fanno inesorabilmente sconnettere dalla rete. È questa la tecnica più utilizzata in assoluto anche in virtù del fatto che è funzionale sia contro utenti singoli sia contro shell o server. L'uso di programmi anti-nuke, l'uso del nuovo protocollo IPv6 e magari di un buon firewall che limiti il raggio d'azione dei malintenzionati, possono essere tutte strategie utili per prevenire attacchi diretti.

Cloni: client aperti da utenti e collegati a server diversi. Si riconoscono facilmente in quanto caratterizzati dallo stesso IP.

>> Dividi et impera

Passiamo oltre ed introduciamo un'altra tecnica di attacco: gli split. Ovviamente sono ben pochi gli utenti in grado di causarne uno, ma tutti possono utilizzarli, quando presenti, per compiere azioni di IRCwar. Questo exploit sfrutta il principio per cui nel momento in cui un server splitta dalla rete ne rimane completamente isolato.



I collide portano ad un kill di entrambi i clienti connessi. Si noti il nick e gli IP dei clienti collidati.

Tutti i client collegati su quel server possono interagire tra di loro ma non con quelli collegati agli altri server, e si viene di conseguenza a creare quella che può essere definita come "rete autonoma". Supponendo che siate moooolto fortunati potrebbe darsi che vi troviate in un server talmente isolato de essere soli all'interno della stanza. Uscendo e rientrando acquisirete automaticamente lo stato di OP. Ora inizia il difficile: al relink del server alla rete voi rientrerete nel chan con lo status di OP, ma ne verrete ben presto privati dai BOT presenti in esso, che in automatico kikkano tutti gli utenti non addati ai loro userfiles. Dov'è il vantaggio quindi? Se anche voi avete una botnet potete farla entrare nel chan splittato, oppare tutti i vostri BOT e sperare che al relink questi siano più veloci o impostati meglio di quelli presenti. Inizierà una guerra a colpi di op/deop fra i BOT e **l'ultimo che rimarrà oppato nel canale vincerà battaglia e controllo del canale.** Visto l'attacco analizziamo la difesa: se come owner di BOT non siete completamente decerebrati magari avrete joinato più BOT su più server diversi in modo tale da eliminare il maggior numero possibile di split dal rischio take. Magari anche entrare per qualche minuto nel server splitatto e dare uno sguardo che nessuno sia OP nella vostra stanza potrebbe risultare utile.

Take: insieme di tecniche che permette di "rubare" un canale al legittimo proprietario.

>> Lei non sa chi sono io...

Ulteriore strategia di attacco, complessa da realizzare e che necessita di molta preparazione, prontezza di riflessi e conoscenze, ma che conduce quasi sempre ad ottimi risultati è il collide + serverOP. Vi è mai capitato di entrare in IRC e vedere nella finestra status il messaggio "Nick già in uso"? Se non vi è ancora successo vi succederà non preoccupatevi! IRC è strutturata in modo che non possano coesistere due utenti con lo stesso nick, per l'ovvia ragione della trasmissione dei pacchetti. Ma cosa succede se in uno split, dove come abbiamo visto si creano due reti separate, si connettono due utenti che hanno lo stesso nick? Al relink ovviamente i server non sono in grado di stabilire chi abbia la priorità e si comportano nell'unica maniera possibile: sconnettono entrambi i client. Su questo principio si basa la tecnica del collide. Ho affermato prima che richiede molte risorse e molto tempo, infatti nel momento dello split l'attaccante deve avere a disposizione un numero più grande possibile di cloni da collegare al server splittato. Darà a ognuno di questi il nick da collidare sulla rete ed aspetterà il relink. Giunti a quel fatidico momento, raggiungerà l'orgasmo guardando la bellissima pioggia di scritte blu con i nick e gli IP dei client collidati e sconnessi. **Se riuscirà a far fuori tutti i BOT e gli OP di un determinato chan, resterà l'unico operatore in esso ed avrà vinto.** Sembra semplice ma credetemi che non è proprio così. Già trovare molti cloni non è facile e poi avere la prontezza di reagire alla varie astuzie messe in atto dagli owner del chan richiede velocità ed idee chiare sul da farsi.

Come sempre, analizzato l'attacco vediamo la difesa: i BOT hanno una funzione interna che se attivata, in caso di split, cicla loro il nick automaticamente impostandolo con caratteri casuali. Questo com'è ovvio complica non di poco il lavoro dei takkatori, lavoro che può essere ulteriormente reso ostico dall'eventuale chiusura del canale con impostazione +i. Al solito, vi suggerisco di fare capolino nel server splittato e con un bel /whois dei nomi dei vostri BOT controllare che nessuno stia caricando cloni per un collide. Comunque sia, il metodo migliore è sempre dare libero sfogo alla vostra fantasia pensate, sperimentate nuove idee e nuove tecniche e vedrete che alla fine riuscirete, se siete OP con un po' di palle con la voglia di lavorare e studiare, a proteggere sempre il canale da attacchi esterni di IRCrompiscatole!

Shell: interprete dei comandi utilizzata in ambiente *NIX

CAT4R4TTA,
cat4r4tta1hackerjournal.it

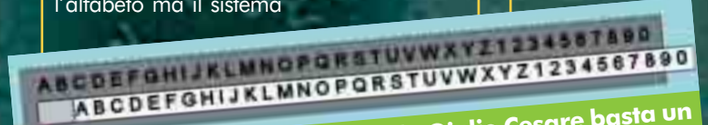
DA GIULIO CESARE ALLA IBM

Da secoli i matematici combattono tra loro una battaglia: da un lato, quelli che cercano di inventare codici di cifratura inviolabili; dall'altra, quelli che fanno di tutto per vanificare gli sforzi dei primi.

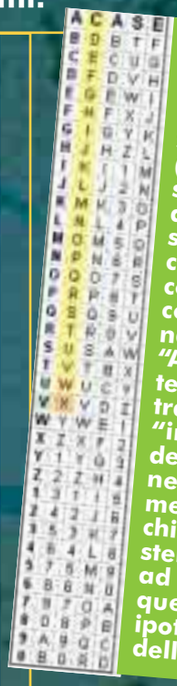
Per capire come funzionano i sistemi di crittografia moderni dobbiamo partire da lontano. Per essere precisi dobbiamo risalire ai messaggi che Cesare inviava alle sue truppe. Per evitare intercettazioni, Cesare scriveva i messaggi traslando le lettere. In sostanza un messaggio con chiave 3 utilizzava un alfabeto secondo il quale A=D, B=E, C=F e così via. Naturalmente un cifrario di questo tipo andava bene solo in epoca romana perché **oggi chiunque è in grado di decifrare un messaggio del genere usando solo carta e penna**. Le chiavi di cifratura, infatti, sono solo 26, tante quante le lettere dell'alfabeto. Naturalmente occorre però scartare la prima perché corrisponde al testo in chiaro (A=A, B=B, ecc..)
Alcuni miglioramenti si ottennero facendo corrispondere lettere casuali alle lettere dell'alfabeto ma il sistema risultava complicato, il cambiamento dei codici era macchinoso e soprattutto l'operazione risultava inutile visto che con un'analisi statistica dei caratteri cifrati era possibile risalire ai caratteri "in chiaro" confrontandone la frequenza con quelli normalmente utilizzati.

>> Complicare le cose

Un'evoluzione del sistema usato da Cesare era chiamato "codice di Vigenere" si basava invece su una tavola quadrata che aveva sulla prima riga il normale alfabeto e su quelle seguenti tutte le combinazioni usate nel cifrario di Cesare. Prima di tutto si doveva scegliere una chiave. Poi si scriveva a ripetizione la chiave sotto al messaggio da cifrare. Per finire si cifrava ogni singola lettera del messaggio utilizzando il codice corrispondente alla riga della lettera della chiave. Per esempio per cifrare il messaggio "Sto mangiando una mela" usando la chiave "camino" si scriveva sotto il messaggio "caminocaminocaminoc". Poi si cifravano singolarmente le lettere secondo le chiavi date dalle lettere della chiave. Per esempio con chiave "c" la lettera corrispondente alla "s" del testo in chiaro è la "u". Alla fine si ottiene una cosa tipo "utaunciimvqwnaurzc" che decodificato con la chiave "camino" e lo stesso sistema ci dà il messaggio originale. Il vero problema di questo sistema venne messo in luce nella metà dell'800 perché si notò che in messaggi lunghi, alcuni



Per interpretare il codice usato da Giulio Cesare basta un semplice righello con una barra scorrevole su cui segnare le lettere dell'alfabeto. Facendo scorrere la parte inferiore si cambia la "chiave" necessaria per la decodifica. In realtà questa operazione veniva spesso fatta manualmente oppure si ricorreva a due ruote fissate sullo stesso perno di cui la superiore più piccola. Ruotando quella più piccola si creavano nuove corrispondenze con quella più grande. Per comprenderlo senza possedere la "chiave" bastava però qualche tentativo con carta e penna.

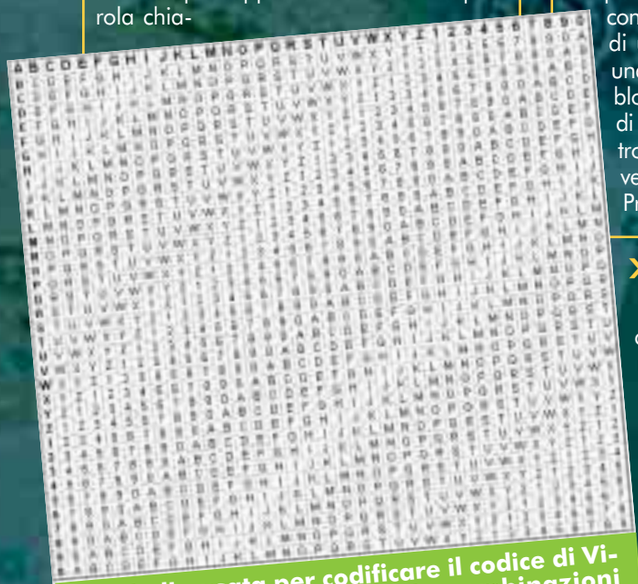


La codifica e la decodifica di un testo con il cifrario di Vigenere è un'operazione banale. Si sceglie una chiave (in questo caso è "case") che si scrive in modo continuo sotto al testo da codificare. Poi si cercano le lettere che compongono il testo da codificare nella colonna corrispondente alla "A" e si trascrive la lettera che sta all'incrocio tra la lettera del testo "in chiaro" e quella della chiave. Oggi viene decodificato facilmente anche senza chiave ricorrendo a sistemi "a forza bruta" o ad analisi sulla frequenza dei codici e ipotesi sulla lunghezza della chiave.

L'ALGORITMO DI IDEA

Il sistema di funzionamento di IDEA è molto simile a quello usato dal DES con la differenza che il testo da cifrare viene diviso in blocchi da 64 bit, ciascuno diviso in altri sottoblocchi da 16 bit. La funzione di "scrambling" usata da DES è sostituita con una funzione che provvede a compiere altre operazioni di XOR, addizioni e moltiplicazioni in base 16. Ogni sottoblocco viene sottoposto a 8 passaggi durante i quali il secondo e il terzo sottoblocco si scambiano di posto.
Risulta interessante invece notare come per l'uso di questo sistema vengano generate ben 52 diverse chiavi. La chiave originaria a 128 bit viene infatti divisa in blocchi da 16 bit che costituiscono le prime 8 chiavi. Poi i bit che compongono la chiave originale vengono spostati 25 bit a sinistra, generando una nuova chiave che viene nuovamente divisa in 8 chiavi secondarie. Il procedimento prosegue con spostamenti e divisioni fino a generare tutte le chiavi necessarie.
Il sistema di funzionamento di IDEA, come quello del DES, è ben conosciuto dalla comunità scientifica e si trova facilmente su Internet usando un qualsiasi motore di ricerca.

caratteri tendevano a ripetersi nella stessa sequenza. Per tradurre un messaggio del genere basta quindi analizzare un testo molto lungo o più testi con la stessa chiave, trovare il massimo comune divisore delle distanze tra le sequenze identiche e avremo trovato la lunghezza della chiave. **Una volta identificata la lunghezza della chiave potremo poi procedere per tentativi nella decifrazione** visto che tutto si riduce a una serie di cifrari di Cesare.
Un altro sistema di cifratura consisteva invece nella trasposizione del messaggio, in un rimescolamento del messaggio secondo una certa chiave. Si sceglieva come chiave del messaggio una parola che non contenesse lettere doppie. Poi si scriveva il messaggio sotto la parola, andando a capo ogni volta che si arrivava al termine della parola.
In questo modo si formavano tante colonne di lettere quante erano le lettere della parola chiave. Poi si trascriveva il messaggio ordinando le colonne trascritte in base alla posizione delle lettere della parola chiave. Per esempio supponiamo di usare la parola chiave "marco" e codifichiamo il messaggio "Oggi sono andato a fare una gita al lago". Sotto la "m" della parola chiave troviamo le lettere "oodfnag". Riordinando alfabeticamente le colonne in base alle lettere della parola chiave avremo un rimescolamento nel messaggio con l'ordine di colonne "a","c","m","o" e "r". Il messaggio risultante sarà quindi "gnaaaaoiaoeiloodfnagsnautagotrgl". Anche se all'apparenza la decifrazione potrebbe sembrare molto complicata, in realtà **è possibile infrangere il codice ipotizzando la lunghezza della chiave andando per tentativi**. La famosa macchina ENIGMA usata dalle truppe tedesche durante la seconda guerra mondiale non era altro che un sistema meccanico di cifratura che usava il metodo appena visto applicandolo più volte a ripetizione e codificando quindi del testo già codificato.
Il DES è il primo sistema di cifratura che viene adottato come standard. Nel 1977, dopo il suo sviluppo da parte di IBM e successive modifiche da parte dell'agenzia di sicurezza nazionale degli USA viene introdotto per la protezione di dati non classificati come segreti di stato o militari. Si tratta di un sistema di codifica che utilizza una chiave di codifica a 64 bit divisa in blocchi da 8 bit ciascuno. L'ultimo bit di ogni blocco viene usato per il controllo dei precedenti e quindi la chiave vera e propria è di 56 bit.
Proprio la scarsa lunghezza della



La tabella usata per codificare il codice di Vigenere raccoglieva tutte le combinazioni possibili del codice di Cesare e le usava insieme ad una chiave per ottenere il codice cifrato. Rimase in uso fino all'800 perché era il codice ottenuto era difficilmente analizzabile. Non fu più considerata affidabile quando si notò che nei lunghi messaggi alcune sequenze di lettere codificate si ripetevano e permettevano un'analisi manuale.

>> DES e IDEA

chiave è stata la sorgente di numerose polemiche in merito alle scelte "guidate" dalla NSA verso l'adozione del DES. Nel 1998 viene annunciata dalla EFF (Electronic Frontier Foundation) la nascita del primo sistema hardware per la decodifica dei messaggi che usano DES. Entro l'anno 2000 il DES diventa storia perché le informazioni per costruire un DES-Cracker sono ormai alla portata di tutti.
Il successore del DES è IDEA, un sistema di codifica simile al DES che però utilizza chiavi di 128 bit. Questo permette di ottenere una maggior sicurezza visto che le possibili combinazioni per la decodifica sono ben 2^128, sufficienti per scoraggiare qualsiasi singolo analista e anche la maggior parte dei governi.

Khamul

L'algoritmo del DES

Il testo da cifrare viene diviso in blocchi da 64 bit. Ogni blocco cambia poi posizione con un altro e diviso in due blocchi da 32 bit l'uno. Poi, per 16 volte, viene applicata una funzione che traspone e fa delle sostituzioni ad ogni metà del blocco utilizzando una chiave ricavata matematicamente dalla chiave originale.Durante ogni passaggio le due metà del blocco si scambiano di posto.
L'algoritmo è ricorsivo e quindi i cambiamenti operati sui dati sono notevoli.

Il blocco totale è uguale al mezzo blocco sinistro seguito dal mezzo blocco destro in un certo passaggio indicato con "n".
T(n)=L(n)R(n)

Il mezzo blocco a sinistra è uguale al mezzo blocco di destra del passaggio precedente (n-1).
L(n)=R(n-1)

Il mezzo blocco di destra è uguale al mezzo blocco di sinistra del passaggio precedente sul quale è stata fatta un'operazione di OR esclusivo (XOR) confrontandoli con il risultato di una funzione che coinvolge la chiave. La chiave viene costruita matematicamente ad ogni passaggio ricavandola dalla chiave originaria. Quindi cambia in continuazione a seconda del valore di n.
R(n)=L(n-1) XOR funzione[R(n-1),CHIAVE(n)]

La funzione appena vista è abbastanza complicata ma non inaccessibile.
Per prima cosa il blocco R(n-1) da 32 bit viene espanso in modo da fargli occupare 48 bit. Su questo blocco espanso viene poi fatta un'operazione di XOR (OR esclusivo) rispetto alla chiave utilizzata per quel passaggio. Il risultato dell'operazione viene spezzato in 8 blocchi da 6 bit ciascuno. Ogni blocco viene poi processato da una funzione che controlla alcune matrici fisse (chiamate S-Box) prelevando da esse delle stringhe di 4 bit identificate in base ai 6 bit di ingresso. Ogni blocco da 4 bit viene poi riagganciato agli altri blocchi scambiandoli di posto tra loro. Il risultato in uscita è un nuovo blocco da 32 bit ma codificato tramite l'operazione di XOR con la chiave e la sostituzione con i valori delle S-Box.

SONO DAVVERO SICURE LE TEXTBOX PER PASSWORD IN WIN98?

Leggere tra le righe

Bastano poche istruzioni in Visual Basic per rivelare la maggior parte delle password nascoste dagli asterischi in Windows.

Quando si deve inserire una password all'interno di una casella di testo, il fatto che al posto del testo compaiono degli asterischi rassicura i più sulla sicurezza di ciò che si sta compiendo. Molti infatti interpretano la presenza di questi caratteri come la certezza di non poter essere spiati, o quanto meno di tenere al sicuro le proprie password.
Poi, per paura di possibili keylogger (programmi che memorizzano tutto ciò che si digita e in che finestra lo si fà, rimanendo in background a spiarci), o solo per pigrizia, la maggior parte delle persone tende a memorizzare le password così da non doverle ridigitare.
Sinceramente ho visto ben poche persone non farlo, soprattutto se normalmente sono gli unici a usare quella postazione. Ma i nostri dati sono davvero dentro ad una fortezza? Di seguito proveremo ad usare due tecniche per scoprire cosa si nasconde dietro ai nostri "amici" asterischi, e vedremo se la fortezza è espugnabile o meno.

>> Tecniche di lavoro

Fatta la premessa mettiamoci al lavoro! Per prima procuriamoci tutto l'occorrente: VB6.0 e apriamo un nuovo progetto su questo IDE. Basta! E' incredibile, ma per aprire la "serratura" della TextBox non serve null'altro.
Vediamo cosa inserire nel form che di default ci appare nel progetto:

Controllo	Nome	Proprietà
TextBox	ClassName	Caption=""
TextBox	WindowName	Caption=""
Timer	Timer1	Interval=10

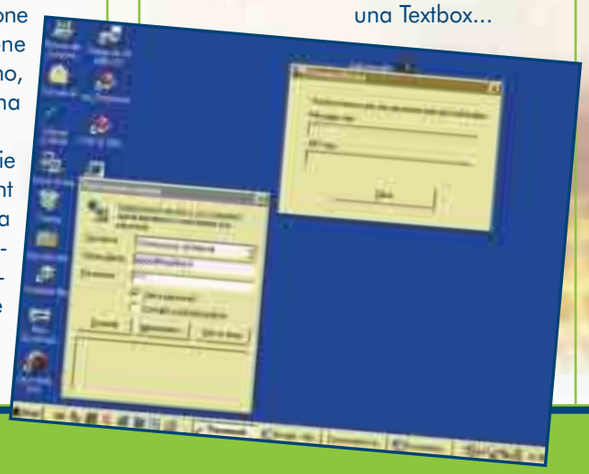
Per seconda cosa dobbiamo andare a dichiarare all'interno di un modulo (un file .bas per capirci) le API che ci serviranno:

```
Public Type POINTAPI
        x As Long
        y As Long
End Type

Public Declare Function GetCursorPos
Lib "user32" (lpPoint As POINTAPI) As
Long

Public Declare Function WindowFromPoint
Lib "user32" (ByVal xPoint As Long,
ByVal yPoint As Long) As Long

Public Declare Function SendMessage Lib
"user32" Alias "SendMessageA" (ByVal
hwnd As Long, ByVal wMsg As Long, ByVal
wParam As Long, lParam As Any) As Long

Public Declare Function GetClassName
Lib "user32" Alias "GetClassNameA"
(ByVal hwnd As Long, ByVal lpClassName
As String, ByVal nMaxCount As Long) As
Long

Public Declare Function GetWindowText
Lib "user32" Alias "GetWindowTextA"
(ByVal hwnd As Long, ByVal lpString As
String, ByVal cch As Long) As Long
```

Combinandole opportunamente, possiamo risalire all'handle della textbox con la nostra password, solo appoggiandovi sopra il puntatore del mouse. Infatti la funzione GetCursorPos ritorna la posizione che il mouse occupa sullo schermo, restituendocela all'interno di una struttura di tipo POINTAPI.
Avuta questa informazione, grazie alla funzione WindowsFromPoint che riceve come parametro una coppia di coordinate, possiamo ottenere l'handle della finestra che risiede sotto al puntatore: sempre che ve ne sia una!
E ora? A molti sarà venuta alla mente l'API GetWindowText. È davvero così facile?
Proviamo inserendo quanto segue nel codice del programma:

```
Private oldHWND, pwdHWND As Long
Private strWindowName As String * 30
Private strClassName As String * 30
Private currentPos As POINTAPI

Private Sub Timer1_Timer()
    Dim Help1 As Long
   currentPos1 = GetCursorPos(currentPos)
      pwdHWND = WindowFromPoint(current-
Pos.x, currentPos.y)
    If oldHWND = pwdHWND Then Exit Sub
    oldHWND = pwdHWND
    HandleNumber.Text = pwdHWND
       Help1 = GetClassName(pwdHWND,
strClassName, 30)
      Help1 = GetWindowText(pwdHWND,
strWindowName, 30)
    'Le seguenti sono le due textbox che
visualizzano il risultato
    ClassName.Text = strClassName
    WindowsName.Text = strWindowName
End Sub
```

Quando si cerca di ricevere il testo presente nella finestra si incorre però in una spiacevole scoperta: se è un bottone, ricevo la sua caption; se è un form, il titolo e se è una Textbox...



IL CODICE DEL RIVELATORE DI PASSWORD

```
Modulo.bas

Public Type POINTAPI
        x As Long
        y As Long
End Type

Public Const EM_SETPASSWORDCHAR = &HCC

Public Declare Function GetCursorPos
Lib "user32" (lpPoint As POINTAPI) As
Long

Public Declare Function WindowFromPoint
Lib "user32" (ByVal xPoint As Long,
ByVal yPoint As Long) As Long

Public Declare Function SendMessage Lib
"user32" Alias "SendMessageA" (ByVal
hwnd As Long, ByVal wMsg As Long, ByVal
wParam As Long, lParam As Any) As Long

Main.frm

Private oldHWND, pwdHWND As Long
Private currentPos As POINTAPI

Private Sub Timer1_Timer()
    Dim Help1 As Long
   currentPos1 = GetCursorPos(current-
Pos)
    pwdHWND = WindowFromPoint(current-
Pos.x, currentPos.y)
    If oldHWND = pwdHWND Then Exit Sub
    oldHWND = pwdHWND
       Help1  =  SendMessage(pwdHWND,
EM_SETPASSWORDCHAR, 0, 0)
End Sub
```

non ricevo nulla.
L'esito è di questo tipo perchè la Microsoft ha ben pensato di nascondere il valore di una casella di testo, altrimenti sarebbe un gioco da ragazzi conoscerne il contenuto.
Se ci fermassimo qua potremmo pensare di essere in una botte di ferro, ma prima di cantar vittoria è meglio provare con un secondo metodo.

» Seconda tecnica

Noi sappiamo che una TextBox di Visual Basic sarà rappresentata a video attraverso un controllo della classe standard di Windows detta Edit. Questo vale per qualunque applicazione ricorra agl'elementi grafici standard del sistema operativo: C++ o Basic che sia. Occorre spendere due parole per Java: questo linguaggio possiede due tipologie di GUI. La prima è legata al S.O. su cui gira la virtual machine (AWT), mentre la seconda è proprietaria delle Api java (Swing) e slegata dal sistema. In entrambi i casi la tecnica appena vista non funziona con il linguaggio della Sun.
Torniamo a noi. I controlli di tipo Edit, a seconda di come vengono visualizzati, fanno ricorso a vari stili. Tra questi stili vi è l'ES_PASSWORD: se è presente ci avvisa che la casella di testo è di tipo password.
Tra i Windows-messages che gli Edit possono processare ve ne è uno che fa al caso nostro: EM_SETPASSWORDCHAR. Grazie a questo noi possiamo selezionare quali caratteri far apparire al posto della parola digitata; normalmente si usa l'asterisco, ma altri potrebbero desiderare il cancelletto, o una ingannevole sequenza di 'a', e via dicendo.
Noi, in fase di spedizione del messaggio, indicheremo quale carattere utilizzare attraverso il parametro wParam della funzione SendMessage. Modifichiamo l'evento Timer come segue:

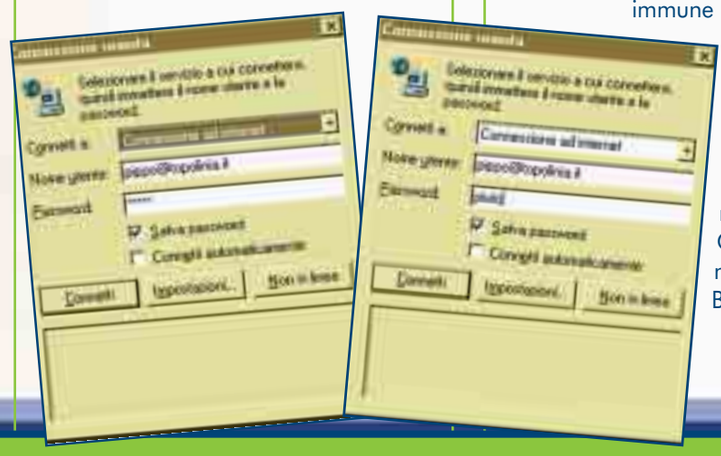
```
Public Const EM_SETPASSWORDCHAR =
&HCC

Private Sub Timer1_Timer()
    Dim Help1 As Long
   currentPos1 = GetCursorPos(cur-
rentPos)
    pwdHWND = WindowFromPoint(cur-
rentPos.x, currentPos.y)
    If oldHWND = pwdHWND Then Exit
Sub
    oldHWND = pwdHWND
     Help1 = SendMessage(pwdHWND,
EM_SETPASSWORDCHAR, 0, 0)
End Sub
```

Al controllo Edit "posteremo" il messaggio visto sopra, e come carattere un bel 0 (N.B. :non '0' tra due apici).
Ora, se ci mettiamo sopra alla password e clicchiamo col mouse, come per magia la password ci appare bella e chiara direttamente al posto degl'asterischi! Perchè? Semplicemente, perchè lo zero è il carattere di default di una normale textBox.
In realtà, in alcune versioni del sistema operativo Windows, se inviiamo il messaggio WM_GETTEXT all'Edit riceviamo il contenuto della casella: questo è molto strano! Infatti inviare il messaggio o usare l'API GetWindowText è tecnicamente la stessa cosa, solo che l'api è limitata nelle finestre obiettivo su cui funzionare, WM_GETTEXT invece no.
In altre configurazioni, comunque, questo messaggio non ha alcun effetto. Dipende dalle classi usate per i controlli da chi ha costruito il Form!
I metodi appena visti sono stati provati con esito positivo su Win9x e WinME, mentre non hanno avuto alcun effetto su una macchina che faceva girare Win2000 Professional e una con XP, ma se qualcuno volesse provarci e poi farmi sapere...

» Precauzioni

Alla fine rimaniamo con l'amaro in bocca. Non siamo vincitori, anzi.
Sicuramente, un utente malintenzionato, creando un programmino di pochi Kilobyte che esegua tutte le tecniche viste sopra (cioè invii entrambi i messaggi), può conoscere le nostre password.
L'aver scoperto questo, comunque, ci deve stimolare a costruirci da soli un buon controllo nascondi-parole e di utilizzarlo nei momenti in cui vogliamo essere un pochino più al sicuro.
Come base d'inizio potremmo pensare di registrare i tasti premuti sulla textbox e di sotituirli con '*', memorizzando quelli veri all'interno di una variabile. Un controllo siffatto è immune da messaggi tipo EM_SETPASSWORDCHAR, e tra gli stili farà apparire quelli di un desolante (per i malintenzionati!) normale Edit.
Comunque questa non è l'unica strada! Buon lavoro.

Loxeo



PROBABILMENTE IL PIÙ FAMOSO, DI CERTO QUELLO COL NOME PIÙ ORIGINALE...

Azioni compiute:

- Visualizza una lista di programmi in esecuzione, con la possibilità di terminare un processo o di farlo partire;
- Cattura audio e video (se al PC infetto è collegata una webcam o microfono);
- Fotografa schermate dal monitor della vittima e le rende disponibili all'attaccante;
- L'attaccante é in grado di caricare o scaricare file di qualsiasi tipo dal PC della vittima;
- Consente ad utenti non autorizzati di cancellare, copiare, leggere o modificare file.
- Manipola il registro di sistema;
- Rende visibili tutte le password del sistema;
- Segnala la presenza in rete del PC colpito.

Tecniche utilizzate:

All'atto dell'installazione, il server di BO effettua queste operazioni:
- Rileva il suo stato: verifica se sono state impostate delle configurazioni con il Boconfig, altrimenti usa quelle di default.
- Inizializza i socket di Windows (Winsock:WSAStartup e WSACleanup) e crea un file windll.dll (nome che può essere scelto con il BOconfig) nella directory di sistema di Windows.
- Sfrutta la funzione API RegisterServiceProcess per farsi registrare come task di sistema, avendo così la capacità di rimanere attivo anche tra diversi login.

La chiave modificata è:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- Si riserva la porta 31337 (o quella che gli è stata assegnata dal Boconfig).
- Si mette in "LISTENING" e attende i comandi che il client gli invia sulla porta di comunicazione assegnata (default 31337).

Mezzi di contagio:

Come per altri cavalli di Troia, viene spedito per posta unito ad altri file o programmi (innocui) per passare inosservato. È possibile tuttavia riceverlo anche prelevando file da siti non proprio raccomandabili.

Verifica del contagio:

Il server di BO si posiziona nella directory di sistema (solitamente c:\Windows\System) come file exe, il cui nome è spesso dato dall'attaccante. Se questo non avviene, il nome predefinito dovrebbe iniziare con UMGR32.
- avviare il programma RegEdit (c:\Windows\regedit.exe):
- accedere alla chiave KEY_LOCAL_MACHINE\SOFTWARE\microsoft\Windows\CurrentVersion\RunServices;
Oppure andare al prompt di Ms-Dos e, nella cartella Windows, usare il comando netstat-an, che mostra tutte le porte chiamante un qualche programma:
c:\Windows>netstat -an
se il risultato è 'UDP0-0.0.031337*:*" significa che qualcuno sta usando la porta 31337, dunque è consigliabile controllare il registro.
Nel caso trovaste BO sulla vostra macchina e voleste conoscerne la configurazione con un editor di testi, aprite il file <server>.exe e andate a controllare le ultime righe.

Se l'ultima in assoluto è "88$8(8,8084888<88d8h8l8p8t8x8\8'8d8h818", allora il server sta utilizzando la configurazione di default.
In ogni caso, nelle linee appena sopra, in questo ordine sono riportati: nome file, descrizione dei servizi, numero della porta usata ed eventuale password che blocca le impostazioni del server, informazioni su eventuali plug-in.

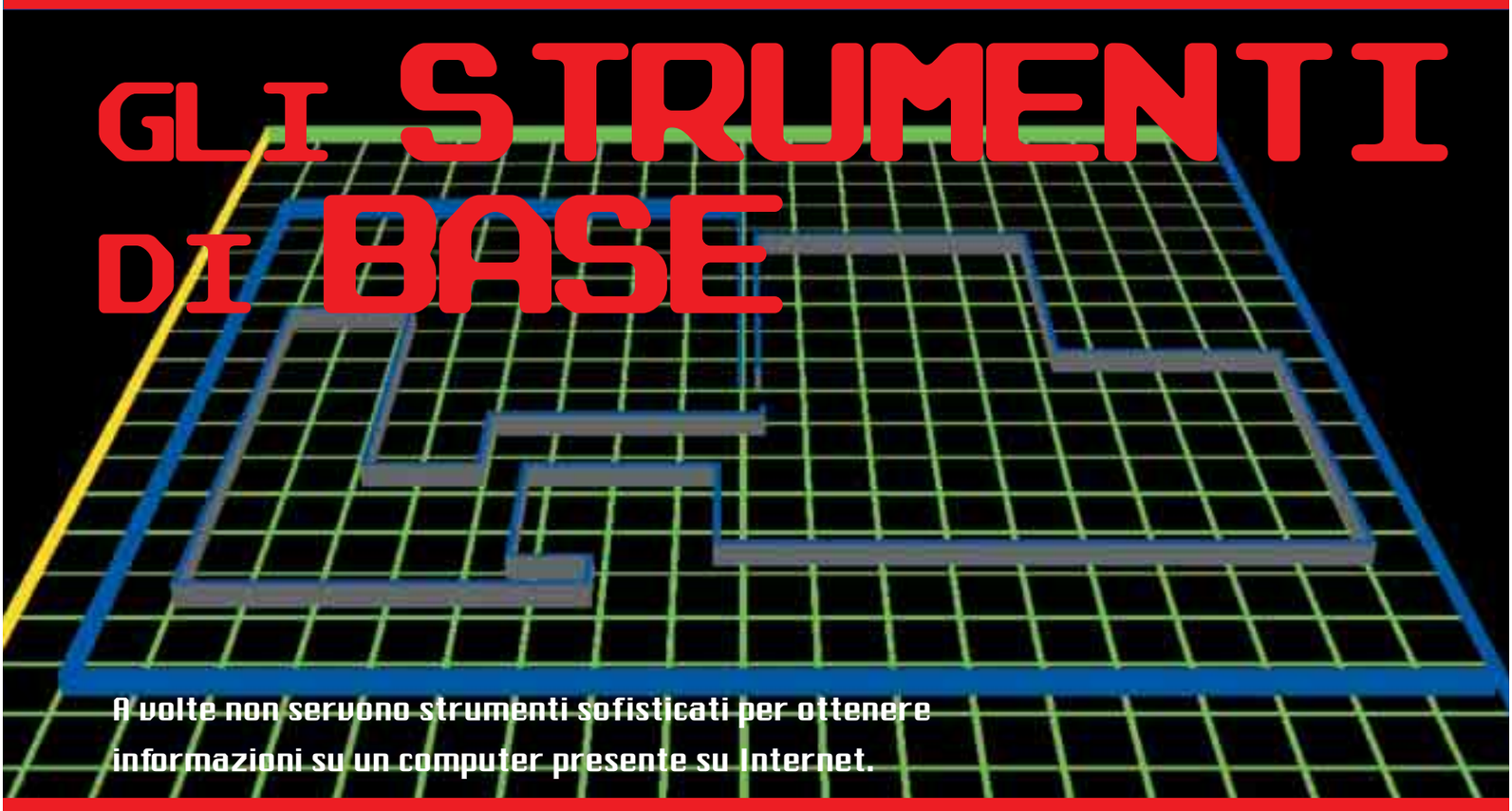
Istruzioni per la rimozione:

Un buon antivirus aggiornato può essere in grado di individuarlo, ma non di rimuoverlo, in quanto non si tratta di un virus. Per questo ci sono appositi programmi come BOdetect (lo rileva e rimuove, la licenza è shareware) o Cleaner (utile per diversi tipi di trojan).

Ulteriori informazioni:

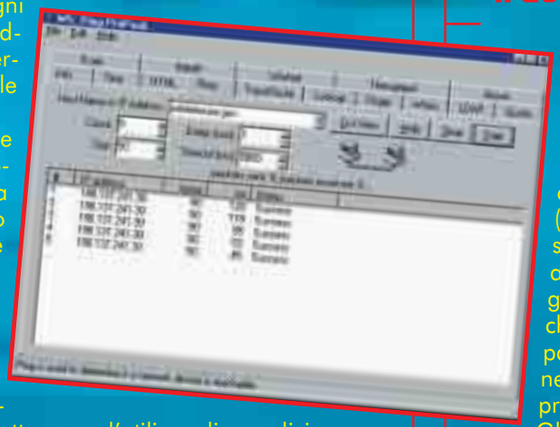
http://securityresponse.symantec.com/avcenter/venc/data/back.orifice2000.trojan.html
http://vil.mcafee.com/dispVirus.asp?virus_k=10002

GLI STRUMENTI DI BASE



A volte non servono strumenti sofisticati per ottenere informazioni su un computer presente su Internet.

Quasi tutte le tecniche usate per le intrusioni si basano principalmente nel reperire il maggior numero di informazioni relative al sito da attaccare; è necessario sapere quali programmi girano sul server vittima (e in quale versione), per poter sapere quale exploit utilizzare in seguito. Anche la tecnica stessa del bruteforce si basa sulla ricerca di ogni dettaglio riguardo l'admin del server per poterne identificare l'eventuale user o pwd.



Per questo, è importante sapere quali informazioni il nostro computer sta distribuendo, nostro malgrado, a chiunque abbia un minimo di capacità e sappia usare un paio di strumenti. E non stiamo parlando di strumenti sofisticati; molte informazioni possono essere recuperati attraverso l'utilizzo di semplici comandi presenti di default su svariati sistemi operativi. Per esempio, installando il protocollo di rete Microsoft TCP/IP, vengono copiati alcuni file in /Windows, questi file sono delle utility per Internet (e reti LAN), che spesso vengono erroneamente sottovalutate.

Tracert Mostra il percorso (HOPS) fatto da un pacchetto per raggiungere un computer remoto.

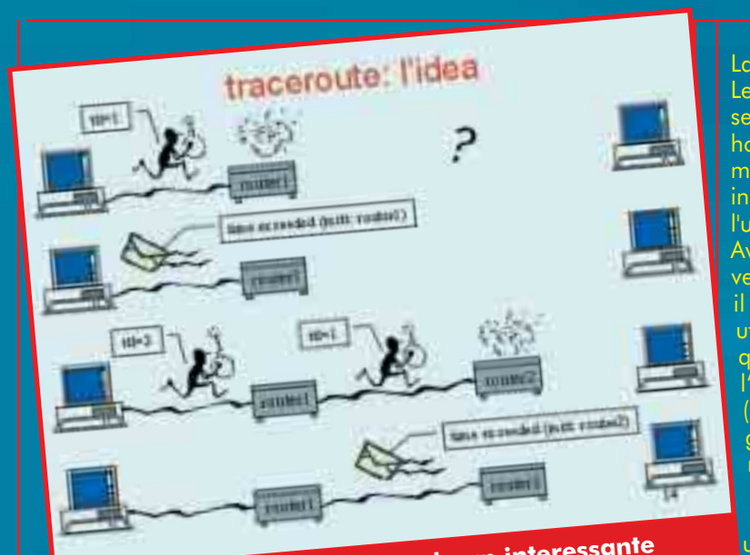
Ping Verifica la connessione di un sito e ne determina i tempi di risposta.

>> Tracert

Si tratta di un'utility che stabilisce il percorso verso una destinazione inviando pacchetti echo con valori variabili di Time To Live (TTL). Lungo il percorso il compito di ogni "instradatore" è quello di abbassare di almeno una unità il TTL di un pacchetto prima di consegnarlo. In pratica il TTL è un conteggio di salti (Hops). Quando il TTL di un pacchetto arriva a 0, l'instradatore dovrebbe mandare indietro un messaggio al sistema di origine. In base ai messaggi rinviati dagli instradatori, viene determinato il percorso del pacchetto. (Acuni instradatori però rendono invisibili i pacchetti echo, lasciandoli esaurire senza che tracert ne rilevi la traccia. Vedremo come affrontare questo problema col comando ping).

Gli switch dei comandi sono case-sensitive, quindi attenzione a come digitate le maiuscole e le minuscole, ad es. è diverso scrivere: Ping -a da Ping -A !!

CONOSCERE PING E TRACEROUTE, DUE UTILI COMANDI



Queste immagini sono tratte da un interessante corso disponibile all'indirizzo www.dia.uniroma3.it/~impianti/HomePage00-01/icmp_ping_traceroute/

Vediamo quindi la sintassi del comando:

```
TRACERT [-d] [-h maximum_hops] [-j host-list]
[-w timeout] nome_destinazione
```

Opzioni:
-d Non risolve gli indirizzi in nome host.
-h Numero massimo di hops per ricercare la destinazione.
-j Libera route di origine lungo l'elenco host.
-w Intervallo di timeout in millisecondi per ogni risposta.
nome_dest Specifica il nome di ospite del computer di destinazione

Facciamo un esempio:

```
C:\windows> TRACERT mbox.virtualbit.it

Rilevazione instradamento verso mbox.virtualbit.it
[195.103.10.3] su un massimo di 30 punti di passaggio:
1 115 ms 121 ms 113 ms 202.41.103.65
2 153 ms 151 ms 149 ms 202.41.103.1
3 192 ms 317 ms 189 ms 202.41.92.10
4 214 ms 188 ms 227 ms [202.41.92.1]
5 186 ms 224 ms 185 ms interbusiness.it [212.41.192.2]
6 * * 2684 ms r-mi3-.interbusiness.it [151.9.15.145]
7 290 ms 234 ms 228 ms r-mi1-fddi.interbusiness.it
                                        [151.99.5.167]
8 402 ms 486 ms 269 ms 195.31.80.134
9 303 ms 795 ms 286 ms 195.103.10.130
10 * 351 ms 512 ms 192.168.0.6
11 756 ms 475 ms 512 ms mbox.virtualbit.it
                                        [195.103.10.3]
Rilevazione completata.
```

[è solo un'esempio]

La prima colonna riporta il numero di TTL (hops).
Le altre colonne indicano i tempi di andata e ritorno in millisecondi per un tentativo di raggiungere l'host remoto. L'ultimo hops è il server da noi analizzato (tin.it), mentre gli hops intermedi sono vari router che instradano il pacchetto. L'asterisco indica che il tempo (timeout) per il tentativo è scaduto, mentre l'ultima colonna riporta il nome e l'indirizzo IP dell'host.
Avrete notato quindi come sia semplice ottenere l'IP di un server tramite il suo nome e viceversa (NSlookup), ovvero trovare il nome del server avendo solamente il suo IP. Infatti possiamo utilizzare tracert su un'indirizzo numerico (IP) e determinare quale sia il provider o il servizio di hosting utilizzato. Da qui l'attaccante potrà avere ulteriori informazioni sulla vittima (anche se ormai quasi nessuno ha una directory pubblica degli utenti, per fortuna). Può per esempio scoprire in quale zona si trova fisicamente il suo computer. Alcuni provider infatti danno ai propri router dei nomi molto espliciti, che rivelano la loro posizione. Prendete per esempio queste lineee tratte da un tracert:

```
 5  zar1-ge-2-0-0.milan.cw.net (208.175.148.113)
 8.19 ms  19.242 ms  6.079 ms
 6  ycr1-ge-3-2-0-0.milan.cw.net (208.175.148.145)
2.673 ms  5.443 ms  12.061 ms
 7  bcr1-so-6-0-0.frankfurt.cw.net (166.63.195.161)
59.839 ms  57.466 ms  63.606 ms
 8  cable-and-wireless-peering.frankfurt.cw.net
(166.63.195.194)  48.79 ms  48.125 ms  48.264 ms
 9  ae0-12.mp2.frankfurt1.level3.net (195.122.136.34)
46.889 ms  48.171 ms  46.391 ms
10  so-1-0-0.mp1.london2.level3.net (212.187.128.49)
45.593 ms  46.552 ms  46.51 ms
11  so-1-0-0.mp1.washington1.level3.net
(212.187.128.138)  121.017 ms  117.968 ms  119.945 ms
12  so-3-0-0.mp2.sanjose1.level3.net (64.159.1.130)
199.863 ms  195.953 ms  192.746 ms
13  gige10-0.ipcolo3.sanjose1.level3.net (64.159.2.41)
199.725 ms  191.748 ms  195.119 ms
```

Più ci si avvicina al computer della vittima, e più dettagliata sarà la posizione geografica. In questo caso, siamo partiti da Milano, passati per Francoforte, fatta una capatina a Londra, Washington per poi arrivare dalle parti di San Jose, in California (le utlime righe sono state omesse).
Tracert quindi comunica a un attaccante informazioni sull'indirizzo e sul provider, insieme al percorso della connessione di rete. Ancora però l'attaccante non sa molto sul server che ha preso di mira; uno dei più elementari sistemi che può utilizzare è il comando ping.

>> Ping

Il comando Ping è utile per controllare un collegamento con l'host remoto e valutarne la velocità. Viene inviato all'host in questione una serie di pacchetti "echo" di 64 byte aspettando i pacchetti di risposta. Questo per quanto riguarda l'utiilizzo canonico e più comune, ma le sue potenzialità non si limitano a questo.

Sintassi:
`PING [-t] [-a] [-n numero] [-l lunghezza] [-f] [-i TTL] [-v TOS]`

Opzioni:
`-t` Ping è eseguito sull'host specificato finchè non viene interrotto.
`-a` Risolve gli indirizzi in nomi host.
`-n` Invia il numero di richieste di echo indicato da numero; il valore di default è 4.
`-l` Invia i pacchetti echo contenenti la quantità di dati indicati in lunghezza; il default è 64 byte;il massimo è 8192.
`-f` Imposta il flag. Non frammenta il pacchetto.
`-i TTL` Imposta la "vita" del pacchetto col valore indicato da TTL
-v TOS Imposta il tipo di servizio col valore indicato da TOS.
`-r` Registra il percorso del pacchetto in uscita e del pacchetto di ritorno nel campo Record Route.
-s Marca orario per il numero dei salti precisati da numero
`-j` host-list Indirizza i pacchetti per mezzo della lista degli ospiti specificata da host-list. Gli ospiti vicini possono essere separati da gateway intermedi.
`-k` host-list Restringe route di origine lungo l'elenco host.
`-w` Intervallo attesa "timeout" (in millisecondi) per ogni risposta.

Facciamo alcuni esempi.

L'IP di un utente è facilmente determinabile in vari modi, il più comune dei quali è probabilmente un contatto in Chat o con un Instant Messenger (Icq, MSN...). Un utente con IP fisso (o al quale venga attribuito un IP variabile in un ristretto range di indirizzi) potrebbe essere identificato anche dai suoi messaggi email o dai post sui newsgroup.
Una volta che l'attaccante ha ottenuto l'indirizzo della sua vittima, può iniziare le sue ricerche.

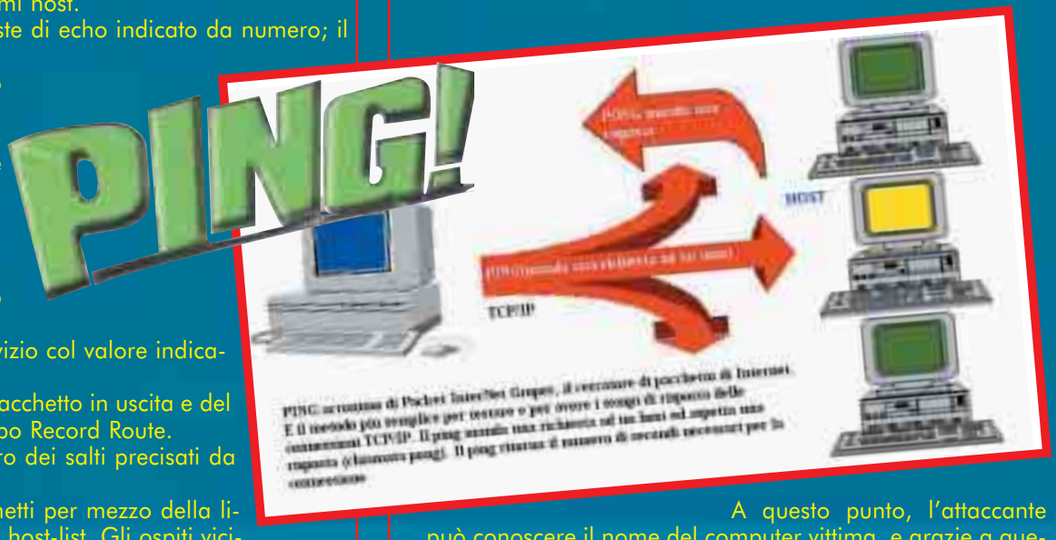
Supponiamo che l'IP della vittima sia 194.105.97.16 (casuale), l'attaccante potrà vedere il nome del computer o l'indirizzo di rete della vittima con:

```
c:\windows> ping -a 194.105.97.16
```

(Sappiamo che il parametro -a risolve un IP num. in nome dell'host)

Il risultato sarà del tipo...

```
Esecuzione di Ping NOME_HOST [194.105.97.16] con 32 byte di dati:
Risposta da 194.105.97.16: byte=32 durata=1ms TTL=128
Risposta da 194.105.97.16: byte=32 durata<10ms TTL=128
Risposta da 194.105.97.16: byte=32 durata<10ms TTL=128
Risposta da 194.105.97.16: byte=32 durata<10ms TTL=128
Statistiche Ping per 194.105.97.16:
Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi: Minimo = 0ms, Massimo = 1ms, Medio = 0ms
```



A questo punto, l'attaccante può conoscere il nome del computer vittima, e grazie a questo essere in grado di rintracciarlo in seguito in qualsiasi momento. Per fare ciò gli serve un DNS-scanner.
Genius per esempio è un programma completo di ogni utility (compreso il ping&tracert appunto). Questa utility permette la scansione di un range di IP; si possono verificare quanti e quali hosts sono online in un intervallo compreso fra due indirizzi.
Prima di andare avanti però apriamo una piccola parentesi.
Come dovreste sapere, l'indirizzo IP assegnato dal Provider ad un'host della sua rete è dinamico, cioè cambia ad ogni connessione, ma la radice (i primi 24 bit) rimane invariata. Se per esempio il vostro IP è 194.10.190.18 significa che appartengo ad un indirizzo di rete :

194.10.190.X dove "X" è il n° host che mi può essere assegnato

(a meno che si tratti di grosse sottoreti, dove l'assegnazione del n° può variare negli ultimi 16 bit --> .192.X e .191.X per esempio). Questo procedimento viene fatto utilizzando una maschera di rete (Netmask) sovrapposta all'IP ... ma questo discorso esula un po' dai nostri scopi (per approfondire, cercate dei testi sul protocollo TCP/IP).
Facciamo un'esempio e torniamo alla nostra vittima in IRC. Supponiamo che l'attaccante era riuscito in precedenza ad avere l'indirizzo IP (per esempio 196.41.197.36) e da questo, con Ping -a abbia scoperto il nome del computer della vittima (quello impostato al momento dell'installazione, o della configurazione di TCP/IP o della condivisione).
In un qualsiasi momento, facendo una scansione della sottorete da 196.41.197.1 a 196.41.197.255, l'attaccante potrà vedere se il nome del computer compare, e associato a quale indirizzo.

MATROX

COME IMPOSTARE MAC OS X PER TENERE FUORI GLI INTRUSI

GIAGUARI IN GABBIA

Una breve introduzione alla sicurezza per Mac OS X, con qualche piccola regoletta che vale anche per gli altri sistemi.

Ok, ammettiamo che fino ad ora non ve ne siate accorti, nonostante il fatto che lo stiamo scrivendo da tutte le parti: il nuovo sistema operativo della Apple, Mac Os X (la "x" significa che è la decima release), è basato su Unix. Cioè, Apple ha celebrato il funerale del vecchio sistema operativo (letteralmente, con tanto di bara e pistolotto di Steve Jobs) ed è ripartita da FreeBSD e Mach. Poi, ci ha messo sopra anche una bella interfaccia grafica, Aqua (rigorosamente senza la "c"), che potremmo paragonare a X-Windows.

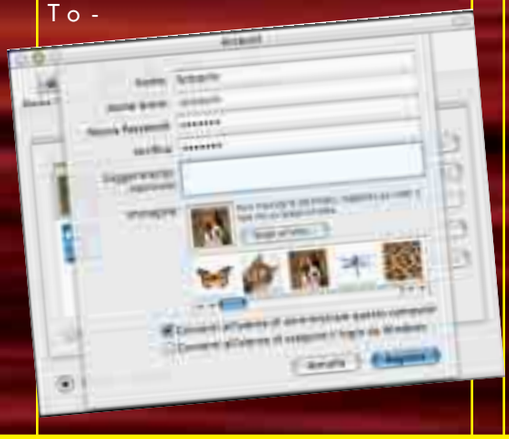
Fin qui, niente di eccezionale, se non il fatto che i programmatori di Cupertino se c'è una cosa che sanno fare, bisogna dirlo, sono le interfacce. Aqua è, oggi come oggi, una bella interfaccia. XP, prodotto da quella azienda di Seattle che non voglio citare, non gli lega neanche le scarpe.

Quindi, ammettiamo che tra chi mi legge ci sia qualche giovane volenteroso, che ha in camera uno stupendo server biprocessore sotto Linux. Questo bravo ragazzo probabilmente vorrebbe anche un portatile, un oggetto adatto da infilare in borsa quando si va in vacanza o alle convention del settore, per amministrare la macchina in remoto ma anche per portarsi avanti con qualche piccolo lavoretto, tipo la gestione del sito etc. Però, sui portatili Linux un paio di problemini ci sono: ad esempio le schede wireless, e amenità del genere, che funzionano un po' a singhiozzo. Non è bello ricompilare ogni due giorni il kernel perché finalmente è uscito il driver (quasi) stabile per il masterizzatore combo-lettore Dvd. Con le macchine di Apple questo non succede (dopotutto è un prodotto commerciale), ma grazie alle fondamenta Unix è possibile fare tutto il resto: dentro ci sono sempre un buon compilatore, GCC 3.1, i vari flavour di C (C++, Objective-C, Objective-C++), Java (1.3.1), Perl (5.60, in attesa del 5.8), Tcl, PHP, Python, Ruby e altro ancora nel più stretto rispetto delle norme POSIX (lo standard comune alle varie release di Unix e Linux). Tutte cose che, stranamente, non si trovano in XP di cui sopra.

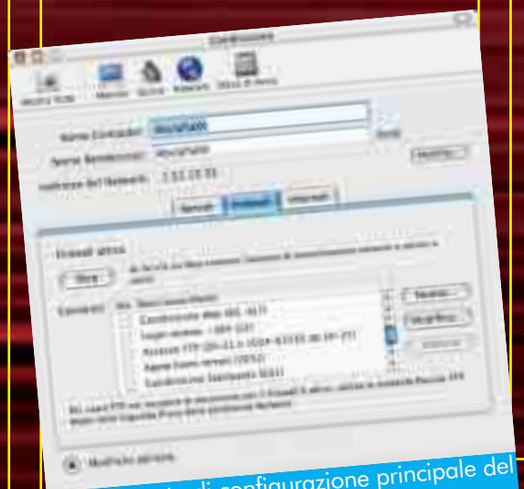
>> Renderlo sicuro

Ma l'interfaccia grafica non serve solo per guardare un Dvd. Se è ben fatta, (e con Mac Os X 10.2.1 lo è), può essere anche utile per fare lavori di amministrazione della propria macchina in modo veloce e preciso. Come front-end grafico, infatti, Os X permette di settare

velocemente i parametri di sicurezza che richiederebbero un lavoro piuttosto duro di editing nella shell.
Vediamo (finalmente) come fare: innanzi tutto cosa ci serve per la sicurezza. Poche regole generali che valgono per tutti e poi alcuni comandi da settare come preferiamo, senza dover digitare neanche un comando testuale nella shell.
Le regole. Una macchina sicura è solo una macchina spenta. Le altre, invece, hanno solo livelli diversi di insicurezza. Vediamo di minimizzarli. Una nota: tenete anche a mente che utilizzo l'inglese come linguaggio del sistema operativo (e quindi nelle schermate in queste pagine). E' un allenamento, perché tante piccole cose che si possono imparare su Internet si trovano in quella lingua. Quindi, perché perdere tempo a tradurre tutto...
Partiamo dall'account. Mac Os X permette di creare tre livelli di account. Uno come amministratore (viene generato durante l'installazione del sistema operativo), uno come utente (generato dall'amministratore) e un super-user, root, che è in grado di fare quello che il normale amministratore non è in grado di fare (come cancellare il sistema operativo). Quest'ultimo si può attivare usando NetInfo Manager (è nella cartella Utility dentro la cartella Applications). Nell'immagine, root è già attivato (ovviamente). Inutile dire che servono tutti e tre e che le password devono essere differenti l'una dall'altra, oltre che non banali. Meglio se lunghe e mescolando lettere a numeri, anziché usando parole di senso compiuto. La prima violazione di una macchina avviene loggando come utente T o -



polino, password Pippo. Là fuori ci sono milioni di tonti che registrano così i loro account. Provare per credere. Ah, evitiamo anche la data di nascita propria o della mamma, mi raccomando.



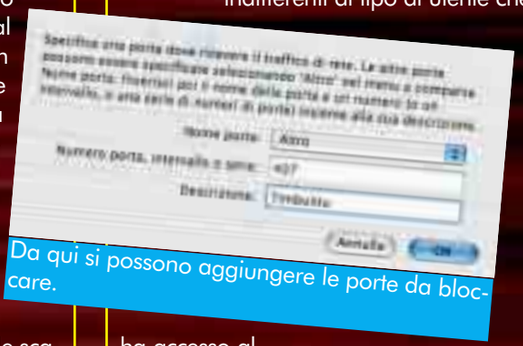
La schermata di configurazione principale del firewall di Mac OS X.

>> La sicurezza fisica

A questo punto, bisogna assicurarsi dagli "assalti" effettuati da persone che possono accedere fisicamente al nostro Mac. Tre piccoli trucchi. Il primo è attivare un qualunque screensaver con richiesta di password. La password è quella dell'account con il quale si è fatto log-in (vedi immagine). Si attiva dal pannello ScreenEffects di System Preferences. La seconda, è attivare la richiesta di log-in all'avvio della macchina. Serve, tra l'altro, ad assicurare che nessuno possa accendere nottetempo il nostro computer e loggare automaticamente come amministratore. Si attiva sempre da System Preferences, pannello Accounts. Terzo, installare una piccola utility di Apple scaricabile dal loro sito, Open Firmware Password, che impedisce al computer di essere avviato utilizzando un cd rom contenente il sistema operativo oppure come single user (premendo la combinazione di tasti Mela-S durante l'avvio, provate per credere).
A questo punto la macchina dal lato "fisico" è praticamente blindata, se solo uno ha l'accortezza di usarla, normalmente, con un account da utente anzichè come root. I privilegi di accesso alla applicazioni e ai file del quale si settano sempre dal pannello Account, cliccando su Capabilities dell'utente designato. Come si può vedere dall'immagine, è possibile restringere parecchio lo spazio di manovra del singolo utente, attivando e disattivando opzioni per l'uso delle applicazioni installate e dell'ambiente generale. Inoltre, le20eventuali applicazioni fatte partire da qualche script sbarazzino vengono bloccate dal livello di sicurezza dell'account e, al limite, richiedono di essere autenticate come amministratore per essere eseguite.
Ok, tutto questo senza usare una riga di testo nella shell, fino ad ora. E anche dopo, sarà così!

>> Condividere, ma con giudizio

Passiamo infatti a capire due concetti importanti. La gestione della condivisione dei file e i settaggi del firewall integrato nel sistema operativo da un lato, e la gestione delle connessioni. Mac Os X presenta un comodo pannello di controllo nel quale settare sia i primi che i secondi. Entrambi questi pannelli sono indifferenti al tipo di utente che



Da qui si possono aggiungere le porte da bloccare.

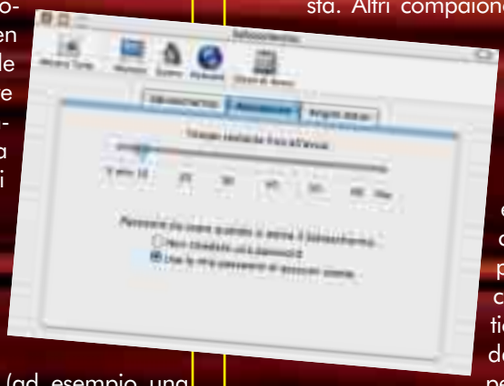
ha accesso alla macchina. Questo vuol dire che se l'amministratore prepara determinati settaggi del firewall, ad esempio, i loro valori influenzano tutti quelli che hanno accesso alla macchina come utenti. Idem per le connessioni.
Le connessioni sono profili differenti, creabili senza limite, attraverso le quali è possibile "navigare" a caldo, cioè passa-

COME IMPOSTARE MAC OS X PER TENERE FUORI GLI INTRUSI

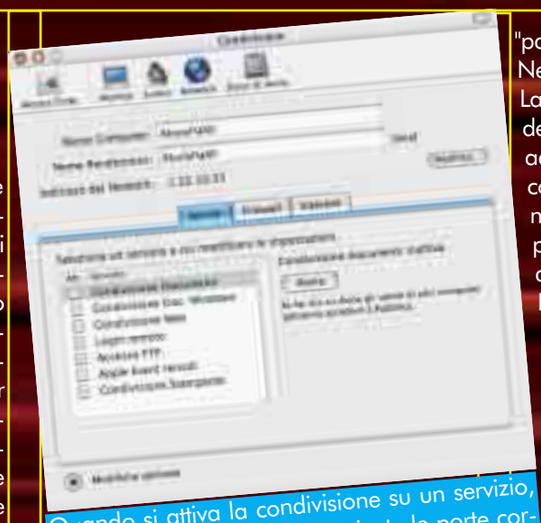
re da una all'altra senza dover riavviare la macchina (hai sentito, Windows?). Questo per un portatile, ad esempio, è molto comodo: senza sofware di terze parti, il computer può attivare modem, scheda ethernet o Airport (802.11b, cioè senza fili) con parametri differenti. I settaggi di ciascun profilo vengono regolati dal pannello Network di System Preferences, ma il passaggio da un profilo all'altro avviene comodamente dal desktop, usando il menu con la piccola Mela (vedi immagine). È una soluzione utile anche per chi abbia diversi account con provider telefonici e preferisca cambiare in modo frequente il suo Isp. Inoltre, ed è importante ai fini della sicurezza, consente di creare un profilo dove ethernet e scheda wireless sono disabilitati via software. In questo modo, si chiudono fisicamente le porte di accesso alla macchina anche se i cavi sono collegati.

>>Il firewall interno

Passiamo infine al firewall, uno degli elementi contenuti nel pannello Sharing. Questo pannello permette (terzo tab) di settare la condivisione dell'accesso a Internet di una macchina con altre collegate (cioè un notevole risparmio sul prezzo di un router), di settare (secondo tab) le regole base del firewall e (primo tab) di settare le regole avanzate di condivisione dei file. In alto, spiccano due strisce: la prima definisce il nome del computer, mentre la seconda ne definisce il nome "Rendezvous", cioè ZeroConfig Technology, uno standard open source accolto da Apple che consente di mettere in rete localmente computer e periferiche senza dover settare ulteriori parametri.



Lasciamo Rendezvous (tanto fa tutto da solo) e partiamo con la condivisione (Services). Se abbiamo un collegamento a Internet fisso (ad esempio una Adsl) o ci colleghiamo a una rete locale per la prima volta, non attiviamo nulla. A meno che non ci serva, e anche in quel caso, chiediamoci se ci serve davvero. Perché concedere l'accesso Ftp alla propria



Quando si attiva la condivisione su un servizio, vengono automaticamente attivate le porte corrispondenti sul firewall.

macchina se non serve? Inoltre, se lo dimentichiamo acceso, altri utenti che possono usare la nostra macchina con account inferiori usufruiranno dello stesso livello di apertura.

Firewall: stessa regola di prima. Se abbiamo un collegamento permanente, facciamo partire il firewall e poi chiediamoci quali porte ci serve che siano aperte, cioè quali tipi di dati possono entrare e uscire dalla nostra macchina. La logica con la quale l'interfaccia grafica di Apple regola il firewall è di esclusione: attivandolo si chiude tutto eccetto i servizi che vengono aperti volontariamente. Alcuni, tra parentesi c'è il numero della porta logica interessata, (vedi immagine)sono già presenti nella lista. Altri compaiono clickando sul pulsante New..., altri ancora li possiamo determinare da zero noi (ad esempio qualche software peer-to-peer come Acquisition, che richiede strani porte per strani collegamenti a strani server...). L'eccezione principale a questo tipo di funzionamento è per l'Ftp, come avverte la stessa Apple: avendo attivato il firewall per scaricare file con l'ftp è necessario attivare l'opzione "passive FTP" nel tab "Proxies" del pannello Network delle System Preferences.

La relazione tra il primo tab e il secondo del pannello Sharing è di tipo logico: se ad esempio attiviamo la condivisione file con Windows (porta 139), automaticamente il firewall ammette l'apertura della porta 139. Per chiuderla, bisogna prima disattivare la condivisione.

Perché tenere tutto chiuso? Certo, se usiamo il Mac senza collegarci a niente, è indifferente. Ma anche su una rete locale un firewall personale è utile, dato che consente di suddividere il rischio di violazioni: se anche viene passato il router con il primo firewall generale, le singole macchine della piccola rete casalinga sono separate. Utile nel caso una macchina sia dedicata a web server (più visibile e maggiormente soggetta a violazioni) mentre con le altre si lavora per altri scopi.

Un'ultima cosa: tramite il pannello Software Update (attivabile anche come comando dalla shell, quindi operabile in remoto) è possibile scaricare con una connessione autenticata gli aggiornamenti del sistema operativo. Tra le altre cose, Apple rilascia gli aggiornamenti di sicurezza per tutti i problemi che possono colpire il kernel BSD o le principali applicazioni. Sono aggiornamenti frequenti (almeno due volte al mese), ed è inutile dire che è meglio installarli subito...

aDm

Occhio alla falsa sicurezza

Quando certe cose vengono troppo semplificate, si rischia di non comprenderle appieno in tutti i loro dettagli. E quando si tratta di sicurezza, non c'è cosa peggiore di avere una sensazione di sicurezza falsa e non corrispondente alla verità. Per stare un po' più tranquilli, non c'è altra alternativa che studiare il funzionamento del firewall interno e personalizzarlo a proprio piaceimento nella maniera più complicata: modificando il file di configurazione. Un interessante articolo su questo argomento è all'indirizzo www3.sympatico.ca/dccote/firewall.html